

国际信息工程先进技术译丛

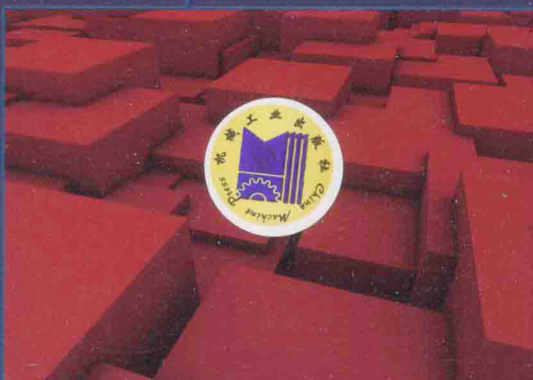
Springer

无线传感器网络——原理、设计和应用

Wireless Sensor Networks: Principles, Design and Applications

[英] 杨双华（Shuang-Hua Yang） 著

张燕 叶成荫 王宏亮 等译



机械工业出版社
CHINA MACHINE PRESS

国际信息工程先进技术译丛

无线传感器网络
——原理、设计和应用

[英] 杨双华（Shuang-Hua Yang） 著
张 燕 叶成荫 王宏亮 等译



机 械 工 业 出 版 社

本书是关于无线传感器网络原理、设计和应用的学术专著，系统阐述了无线传感器网络的原理，深入探讨了设计过程和应用实例。本书内容包括，无线传感器网络的原理、硬件和嵌入式软件设计、路由策略、汇聚节点位置的优化布局、与 IEEE 802.11b 系统的互扰抑制、传感器数据融合与事件检测、安全防御、移动目标的定位与跟踪、面向物流管理的无线射频识别与无线传感器网络的混合网络、物联网，以及智能家居系统和建筑物消防安全防护。

本书面向的主要读者是在校大学生，其次是研究和开发人员。本书也适合任何有兴趣深入了解无线传感器网络的读者。

Translation from English language edition:
Wirelesss Sensor Networks: Principles, Design and Applications
by Shuang- Hua Yang

北京市版权局著作权合同登记图字：01-2014-3876 号。

图书在版编目（CIP）数据

无线传感器网络：原理、设计和应用/（英）杨双华著；张燕等译. —北京：机械工业出版社，2015.4
（国际信息工程先进技术译丛）
书名原文：Wireless sensor networks: principles, design and applications
ISBN 978-7-111-49570-3

Ⅰ.①无…　Ⅱ.①杨…②张…　Ⅲ.①无线电通信-传感器　Ⅳ.①TP212

中国版本图书馆 CIP 数据核字（2015）第 046397 号

机械工业出版社（北京市百万庄大街 22 号　邮政编码 100037）
策划编辑：刘星宁　责任编辑：刘星宁
责任校对：纪　敬　封面设计：马精明
责任印制：刘　岚
北京中兴印刷有限公司印刷
2015 年 5 月第 1 版第 1 次印刷
169mm×239mm · 16 印张 · 329 千字
0 001—2 800 册
标准书号：ISBN 978-7-111-49570-3
定价：68.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务	网络服务
服务咨询热线：010-88361066	机 工 官 网：www.cmpbook.com
读者购书热线：010-68326294	机 工 官 博：weibo.com/cmp1952
010-88379203	金 书 网：www.golden-book.com
封面无防伪标均为盗版	教育服务网：www.cmpedu.com

译 者 序

《无线传感器网络——原理、设计和应用》（Wireless Sensor Networks：Principles, Design and Applications）由国际知名学者、英国拉夫堡大学（Loughborough University）教授杨双华（Shuang-Hua Yang）所著，是一本将无线通信原理与实际的无线传感器网络设计过程相融合的专著。它不仅阐述了无线传感器网络的原理，而且通过物联网、智能家居系统等实际应用提供给读者技术实现的细节，有利于读者独立实现书中的研究工作，并结合自身实际充分利用书中最新技术成果，构建出满足实际需求的解决方案。

本书汇集了作者多年潜心研究的成果，书中论述的内容和观点是作者提出并直接参与设计的，已经由工业界实际验证并得到认可，为物联网相关技术解决实际工程问题提供技术支持和保障。本书不仅可以作为相关专业本科生、研究生的教材，也可作为对无线传感器网络技术感兴趣的研究人员和项目开发人员的参考书。因此译者希望通过翻译工作，将本书的先进理论和技术应用成果奉献给国内相关领域的科研工作者和工程设计人员，有助于我国无线传感器网络的设计和应用工作的开展。

2013 年，杨双华教授应邀来辽宁石油化工大学讲学，我们有幸与杨双华教授讨论了无线传感器网络的若干问题，深化了对无线传感器网络设计与应用的认识。并且，在翻译过程中，我们得到杨双华教授的直接指导和帮助，与杨教授商定了目录和名词术语的翻译，杨教授还审读了翻译初稿，提出了宝贵的建议。本书主要由辽宁石油化工大学张燕、叶成荫、王宏亮翻译，参加翻译工作的还有冯锡炜、王福威、刘琳琳、王晓蕾、题潇颖、李洪兰、石元博、王维民、王晓虹、李楠。另外，本书的翻译工作还得到了国家自然科学基金项目（6120 3021）、辽宁省高等学校优秀人才支持计划（LR2013015）的资助，在此表示感谢。

在翻译过程中，我们曾遇到了一些国内尚未见到或尚无统一译法的名词，斟酌选用了比较能表达其含义的译法，这些译法是否恰当，仍有待业内探讨。由于译者水平有限，翻译不妥之处在所难免，恳请读者批评指正。

译 者

2014 年 12 月

原书致谢

献给我的家人，我美丽的妻子丽丽和我的两个聪慧的儿子杨博和杨健。

并以此纪念于2010年8月过世的我的父亲杨新生先生。

原书前言

无线传感器网络（Wireless Sensor Network，WSN）因为低速率、低能耗和短程连接网络的特性，能以前所未有的规模和分辨率来监视和控制物理世界，越来越成为大规模跟踪和监控应用的解决方案。大量可采样、处理和传输信息到外部系统（如卫星网络或因特网（Internet））的小型、无线传感器的配置应用，开启了许多崭新的应用领域。WSN的潜在应用包括工业控制和监测、智能家居和消费电子、安全和军事传感、资产跟踪和供应链管理、智能农业和健康监测等。美国麻省理工学院（Massachusetts Institute of Technology，MIT）将WSN界定为改变世界的十大新兴技术之一。物联网（Internet of Things，IoT），在技术上得到WSN和其他相关技术的支持，2009年中国已将其列入国家经济发展战略新兴产业之一。WSN的研究主要集中在能耗、路由、容错、数据采集和操作系统，特别侧重于收集和汇总与汇聚节点（又称为WSN网关）相关联的特定网络的数据。一些关于单一或多种应用的异构传感器网络的连接的研究已经开展起来。文献记载最多的主要是可扩展性问题、可靠性、安全性、覆盖范围和大规模配置的相关研究。

本书专注于基于ZigBee的WSN的设计和应用研究，给出了我们过去几年研究和开发工作的第一手资料。本书的一个原则目标是全面覆盖大学课程的相关主题。本书是我指导的9位博士研究生的研究成果和一些公共资助项目研究成果的总结。本书的一个显著特点是，呈现给读者足够的技术细节，让他们能够实际重复实现我们的研究工作而不是仅仅理解背后的原理。我希望这是一个对于工业设计及大学教学和学术研究有价值的参考书。我相信广泛的目标受众是本书具有吸引力的原因之一，因为大部分目前非常有限的已经出版的无线传感器网络书籍主要用于学术研究或作为教材，阐述的是基本概念和原理，较少提供实际设计过程的指导。本书的独特之处就在于同时提供了无线通信原理和实际的WSN设计流程，以促使读者能够利用在本书中学到的技术做新的开发，并应用到他们自己的研究或工业项目中。

本书由3个部分组成，共计15章：第1部分（第1、2章）提供了WSN的原理；第2部分（第3~9章）专注于提供各种设计问题的解决方案；第3部分中的第10~12章探讨WSN在室内位置跟踪、物流管理及物联网的应用技术，紧接下来的第13、14章提供了智能家居系统和建筑物消防安全防护的真实应用实例，第15章是本书结论。

目标受众

本书既可作为教科书也可以作为参考书使用。本书的主要目标读者是在校大学生，书中引用的材料已经作为无线传感器网络理学硕士的教学讲义多次使用，学生

的反馈也包含其中。本书的目标读者还包括相关领域的研究和开发团队，既包括来自学术界的学者，也包括科研院所与产业开发的研究者。本书也适用任何有兴趣深入了解 WSN 领域，但却一直无法找到现实生活中的无线传感器网络设计资料的读者。

致谢

很多人已经直接或间接参与了本书内容的编撰工作。第 3 ~ 12 章根据我以前学生的博士论文编撰而成，他们是姚方博士、卢欣博士、Hesham Abusaimeh 博士、杨燕宁博士、Khusvinder Gill 博士、Tareq Alhmiedat 博士、杨焕甲博士和徐冉博士，以及近期完成博士学位论文的博士研究生 Md Zaid Ahmad 先生。我以前指导的访问学者夏伯楷教授、秦元庆博士及付贵增先生，我以前的研究助理 Donato Salvatore 先生，以及在读的博士研究生何薇薇女士和 Hakan Koyuncu 先生也参与到了本书的编撰工作。我非常感谢他们的辛勤工作和合作。我还要向来自 con- sortiums SafetyNET (DCSI、Sure Technology、Jennic、Arqiva 和 ASFP)、In- deedNET（Advantica、Sure Technology、EMHA）和 iNET 项目（IDC）的工业合作伙伴们；向我的学术合作者浙江工业大学的王万良教授，华中科技大学的周纯杰教授，中国石油大学的田学民教授、夏伯楷教授，辽宁石油化工大学的李平教授，北京理工大学的陈杰教授和清华大学的袁宏勇教授，英国德比（Derby）大学的吴敏宏教授，表示真挚的谢意。有太多需要感谢的人，包括 TSB 项目监测官员 Guy Hirson（SafetyNET）先生和 Mike Patterson（IndeedNET）先生，他们对我们的研究给出了建设性的指导意见；还有我在英国拉夫堡大学计算机科学系的同事们，感谢他们的热情和敬业的协助。

我还要感谢我的同事 Roger Knott 博士和 Charlotte Cross（Springer- Verlag）女士对本书的校对，以及前博士研究生徐冉博士为本书所做的图形设计。

最后，我衷心感谢技术战略委员会通过技术项目（TP/J3521A，TP/3/PIT/6/I/16993）、碳联合信托公司、欧洲区域发展基金的运输 iNET 项目、EPSRC 的通过数字创新的能源转化需求项目（TEDDI）下的能源项目（EP/I000267/1）、中国自然科学基金的重大国际合作项目（61120106010），以及清华大学主持的青年教师和研究人员合作交流 Santander 项目对我工作的资金支持。

杨双华教授

2013 年 7 月

目 录

第1章 绪 论

关键词： 无线通信 无线传感器网络

1.1 无线通信技术

计算机网络已经成为我们日常生活，商业和教育非常依赖的重要组成部分。不管资源或用户的物理位置如何，网络对网络中的任何人都提供信息和服务。计算机网络可以划分成很多类型，如个人局域网（Personal Area Network，PAN）、局域网（Local Area Network，LAN）、城域网（Metropolitan Area Network，MAN）和广域网（Wide Area Network，WAN）。顾名思义，个人局域网就是围绕个人组建的计算机网络；局域网连接计算机的范围小到一个或几个建筑物；而连接一个城市或城镇的网络就叫做城域网；广域网连接计算机的范围大到一个国家或一个洲。这些网络的通信链路通常是有线的，即使用物理线缆连接不同的网络设备。虽然有线计算机网络提供可靠的数据传输，但是其安装成本高，而且在许多情况下安装不便。为了克服这些困难，采用无线通信技术是一个明显的解决方法，尽管无线通信也面临来自自身的如干扰、可靠性及其他因素等的一系列挑战。

无线网络通过无线电波、红外线或其他无线媒体连接设备或计算机。如果无线网络的覆盖范围较大则称为无线广域网；反之，如它的覆盖范围小到一个建筑物则称为无线局域网（Wireless LAN，WLAN）。此外，将个人范围内的信息设备进行互联的无线网络，称为无线个人局域网（Wireless PAN，WPAN）。低速率的无线个人局域网（Low-Rate WPAN，LR-WPAN）是针对低成本、低功耗、短距离无线通信而设计的。

现有的各种无线通信标准包括 ZigBee、Wi-Fi、WiWAX、GSM[⊖]等。图 1.1 给出了各种无线通信标准及特点，并进行了简单比较。这些标准根据支持的流量、通信范围及应用领域进行了分类。例如，Wi-Fi、WiWAX、超宽带 Ultra WideBand 和 802.11a/g/n 通常用于高数据流量的应用，并且通常需要一个主电源。基于 GSM 构建的系统、通用分组无线业务（General Packet Radio Service，GPRS）、增强型数据速率演进技术（Enhanced Date Rate for GSM Evolution，EDGE）、通用移动通信系统（Universal Mobile Telecommunication System，UMTS）和高速下行分组接入

⊖ GSM：Global System for Mobile Communications，全球移动通信系统。

（High-Speed Downlink Packet Access，HSDPA）旨在实现全面的移动性。蓝牙标准的开发主要是为替代计算机互联的网线。ZigBee 标准的开发主要用于无线传感器网络。

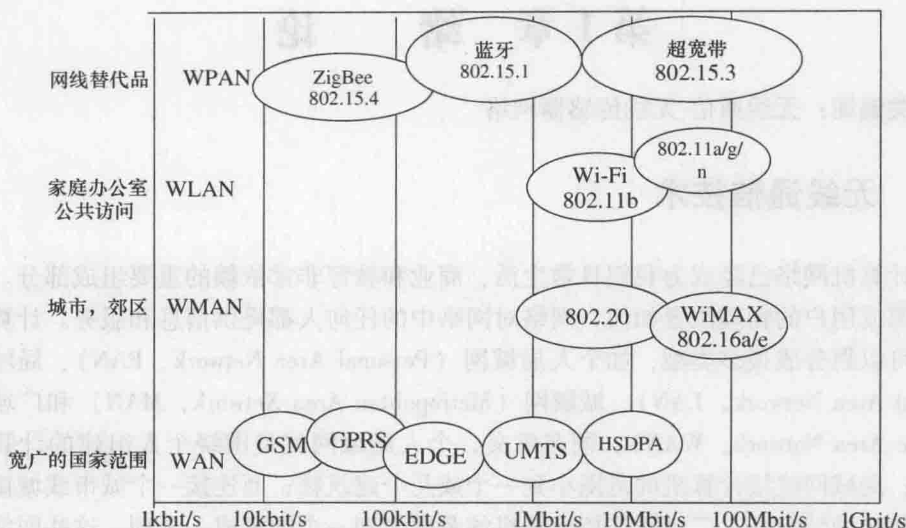


图 1.1 各种无线通信标准及特点（Benini 等，2006）

1.2 无线传感器网络

无线传感器网络（WSN）是由一组具有无线通信基础设施的自治传感器和执行器组成的，旨在监视和控制不同位置的物理或环境条件，并通过网络以协作的方式，将数据传递给一个主位置或将控制命令传递给期望的执行器（Yang 和 Cao，2008）。本书缩小了典型的无线传感器网络的研究范围，即限定数据通信是低速率的，通信范围是短距离的，以及单个传感器节点的物理尺寸小、功耗低和成本低。一个无线传感器网络是由几个或几百个甚至上千个节点组成的，每个节点与一个或多个其他节点相连。节点可设计成具有下面的一个或多个功能——感知、数据中继与外部网络交换数据。用于感知数据的节点称为传感器节点，用于中继数据的节点称为路由器，用于和其他网络交换数据的节点称为基站或汇聚节点，它类似传统网络中的网关。

每个传感器节点负责对监测到的自然现象和环境变化产生电信号。微处理器负责处理和存储传感器的输出数据。无线收发器带有一个内部天线或连接一个外部天线，负责从中心计算机接收命令并将数据传送给中心计算机。图 1.2 给出了典型的无线传感器网络。数据由传感器节点进行汇集，然后传输给连接到因特网或卫星网络的汇聚节点。经过因特网和卫星网络，汇集的数据最后由应用接收。传感器节点

不必有固定的位置，大多数传感器节点随机部署以便监控监测区域。传感器节点通常通过内置无线收发器进行互相通信。

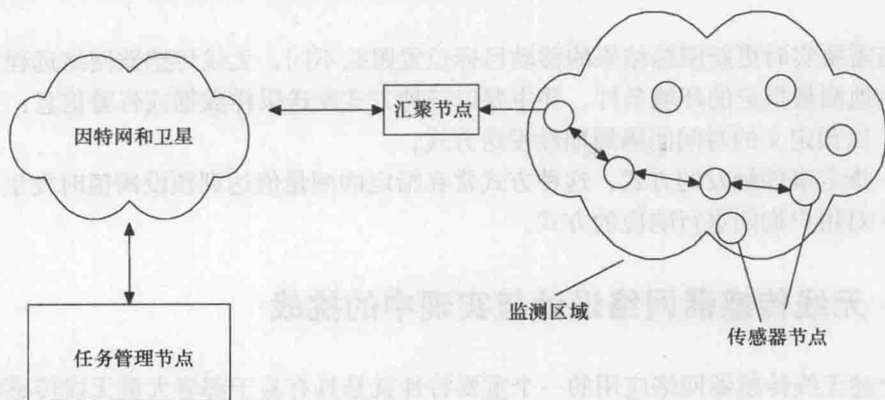


图 1.2　典型的无线传感器网络（Akyildiz 等，2002）

1.3　无线传感器网络的应用领域

无线传感器网络应用可以分为两类：远程监测和移动目标位置跟踪。两者均可进一步分为室内和室外应用。图 1.3 尽可能地给出了无线传感器网络应用的分类，基本上与 Yick 等人（2008）给出的类似。军事应用包括友军监测、敌军活动跟踪、

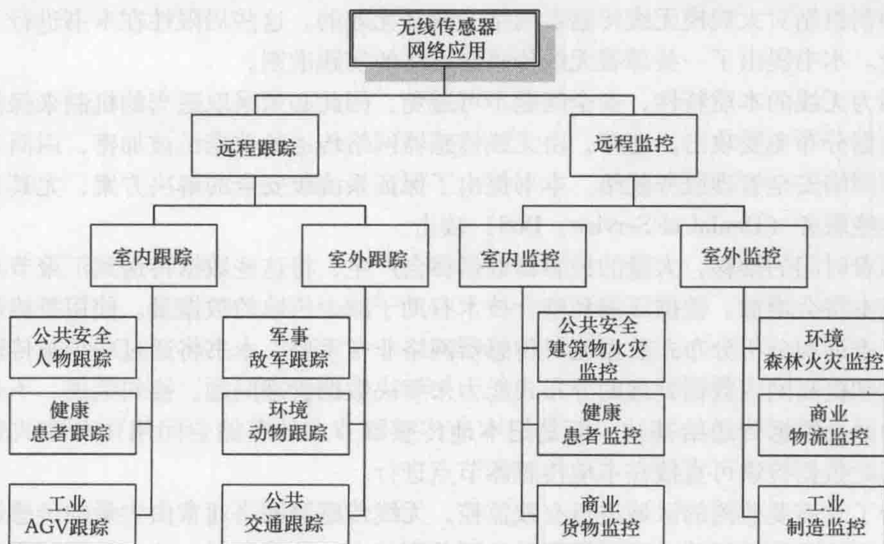


图 1.3　无线传感器网络应用的分类

装备状态检查，或核、生化攻击侦测。环境应用包括动物活动跟踪、森林和建筑物火灾侦测及化学材料泄漏监测。商业/物流应用包括车辆和目标跟踪及库存监控等。

与需要实时更新跟踪结果的移动目标位置跟踪不同，无线传感器网络远程监控周期性地测量指定的环境条件，并主要以三种方式发送采样数据或告警信息：

- 以预定义的时间间隔周期性发送方式；
- 指定事件触发的方式，这种方式常在指定的测量值达到预设阈值时发生；
- 对用户询问进行响应的方式。

1.4 无线传感器网络设计与实现中的挑战

上述无线传感器网络应用的一个重要特性就是具有易于部署大量无线传感器节点的能力。这个特性引起了无线通信通常所涉及的设计与实现的挑战，以及特定应用独有的挑战。其面对的主要挑战包括节能、互扰、安全、数据管理和大规模部署。无线传感器网络的设计与实现必须处理所有这些问题。

节能问题可以用不同的方法解决。一种方法是对硬件和嵌入式软件设计进行优化，如路由算法。路由算法可以使能耗最小化从而提高无线传感器网络的效率。本书从硬件和网络的角度通过优化电源管理解决了节能问题。

由在相近频段工作和同一区域共存的其他无线系统引起的互扰有可能极大地降低无线传感器网络的性能。由于无线传感器网络计算能力低这样的局限性，通常的互扰抑制机制对大规模无线传感器网络一般是无效的。这些局限性在本书进行了充分讨论。本书提出了一些部署无线传感器网络的实践准则。

因为无线的本质特性，安全问题不可避免，因此必须采取适当的机制来保护健全的数据分布免受攻击。通常，由无线传感器网络传送的数据已被加密，因而无线传感器网络安全管理服务就绪。本书提出了保证系统级安全的解决方案，尤其关注远程拒绝服务（Denial of Service，DoS）攻击。

随着时间的推移，大量的传感器数据将会产生，将这些数据传送到汇聚节点的传输成本将会增加。数据压缩和整合技术有助于减少传输的数据量。使用鲁棒策略管理、查询和分析分布式数据流对传感器网络非常重要。本书将通过减少被传输的数据量和提高网内数据处理的分布式能力来解决数据管理问题。换句话说，不是把大量的原始数据传送给基站，而是把本地传感器节点的存储空间用作分布式数据库，因此数据检索可直接在本地传感器节点进行。

为了对需要监测的区域进行有效监控，无线传感器网络通常由大量的传感器节点组成。这些传感器节点可以很容易地覆盖到较大的地理区域。这一特点使得用户无法以手工的方式维护整个网络。因此需要一个综合管理架构来监测无线传感器网络，配置网络参数，以及实现系统更新。当无线传感器网络的规模增长时，可扩展

性问题会降低系统的性能。本书中的应用部分对大规模实现中出现的严重问题进行了监测。仅当节点数限制在100个以内时，这样的实现技术才能有效工作。超出这个限制，阻塞和极大的路由成本极大地降低数据通信速度，并最终中断系统的运行。这个问题在本书的应用技术部分进行了阐述。

1.5 本书的目标

本书旨在作为高年级本科生和研究生的参考书或教材，也可作为无线通信技术研究人员的参考书。本书对软件和系统工程师、公司经理及打算实现无线传感器网络的IT专业人士也是大有裨益的。所以，本书的出发点就是探究无线传感器网络的原理、设计和实现问题，以及研究本领域的设计过程和实际应用问题。本书不同于本领域的其他书籍。那些书籍对IEEE 802.15.4标准和ZigBee标准进行了深入阐释，但缺少系统级的解析和实证（Elahi和Gschwender，2009）。本书也有别于其他一些理论著作。那些理论著作仅呈现了有限的独立主题的研究结果，缺乏系统设计和应用实施的重点（Misra等，2009）。本书的目标是使读者在阅读完本书后能设计和实现自己的无线传感器网络应用。

参考文献

Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cyirci, E.: A survey on sensor networks. IEEE Commun. Mag. **40**(8), 102–114 (2002)

Benini, L., Farrella, E., Guiducci, C.: Wireless sensor networks: Enabling technology for ambient intelligence. Microelectron. J. **37**(12), 1639–1649 (2006)

Elahim, A., Gschwender, A.: ZigBee Wireless Sensor and Control Network. Person Education, USA (2009)

Misra, S., Woungang, I., Misra, S.C.: Guide to Wireless Sensor Networks. Springer, Berlin (2009)

Yang, S.H., Cao, Y.: Networked control systems and wireless sensor networks: Theories and applications. Int. J. Syst. Sci. **39**(11), 1041–1044 (2008)

Yick, J., Mukherjee, B., Ghosal, D.: Wireless sensor network survey. Comput. Netw. **52**(12), 2292–2330 (2008)



第 2 章　无线传感器网络的原理

关键词： IEEE 802.15.4　ZigBee　6LowPan　无线传感器网络

2.1　引言

无线传感器网络（WSN）是无线网络应用的一个子集。WSN 一般不需要使用有线对传感器和执行器进行连接（Gutierrez 等，2004）。由于“无线传感器和执行器网络”或者“无线传感器和控制网络”的名字过长，大多数人都愿意使用“无线传感器网络”这个较短的名字。在任何情况下都要记得，设计这类网络是为了从无线传感器收集信息，并将控制指令发送到与无线网络相连的执行器。

传感器和执行器网络已具有几十年的历史。基于计算机的控制系统是一个典型的固线式传感器和执行器网络。如图 2.1 所示，传感器和执行器通过数据总线系统或其他网络与中央计算机或控制终端连接，实现控制和监视功能。这种类型的固线式传感器网络简单可靠，常见于工业控制，如过程控制和工业生产控制。由于有线传感器网络安装时需进行大量的布线，因此有线传感器网络很难进行扩展。固线式

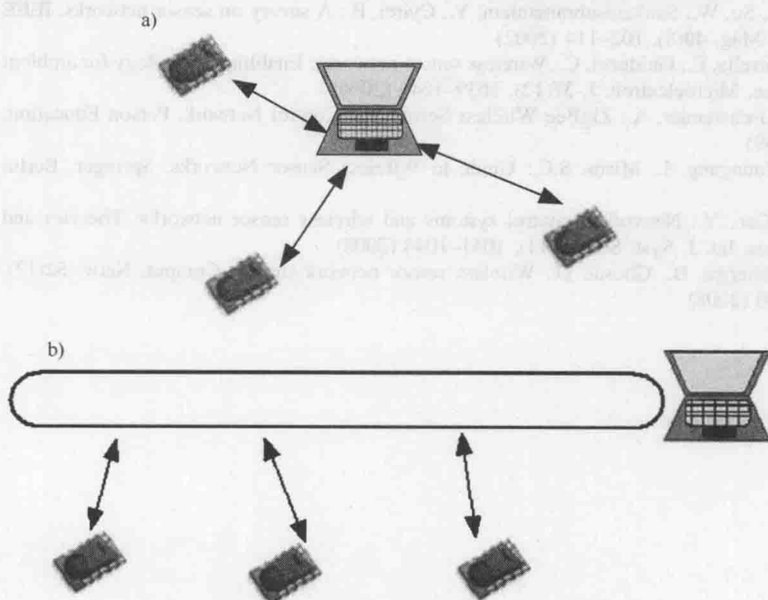


图 2.1　固线式传感器和执行器网络

a）星形固线式传感器和执行器网络　b）数据总线型固线式传感器和执行器网络

传感器网络的安装成本较高，主要表现在布线、人力、材料、测试和验证方面。此外，布线需要的连接器可能会松动、丢失、错接甚至损坏。与广域网络中的存在的问题类似，这个问题常被称作最后一公里连线问题。

将大量固线式传感器网络应用到系统中会给系统带来极大的复杂性，如布线、电力供应和配置。这些复杂性使得固线式传感器网络无法在如森林监测和战地监视方面实施。近年来，集成电路（Integrated Circuit，IC）和微机电系统（Micro Electro Mechanical System，MEMS）的发展成熟使得将无线通信、传感器和信号处理集成在一个低成本的称为传感器节点的模块内成为可能（Schurgers 和 Srivastava，2001）。这样的传感器节点具有数据处理和通信的能力。这些传感器节点的集合就构成了一个 WSN。现在，在许多环境下部署超小型传感器节点来收集信息已成为可能。传感电路测量传感器所在环境的周围情况，并将其转换为可测量信号。该信号经过必要的处理，然后通过无线发射机发送到预定目标。由于传统电源（即电力网）可能不易获得，以上所有操作都由电池来供电以简化部署。

这种传感器网络的无线解决方案具有灵活的连接方式、易于部署。传感器的感知范围决定了 WSN 的应用范围。大部分传感器的类型取决于感知目标的类型（Lewis，2004；Akyildiz 等，2002）：

- 温度
- 湿度
- 声波
- 车辆运动
- 光照条件
- 压力
- 土壤组成
- 噪声
- 某种对象是否存在
- 物体的机械应力
- 物体的目前特征，如速度、方向和大小

此外，无线传感器网络还很多应用，例如以下几方面：

- 监控环境和状态的连续感知
- 灾难应急事件检测
- 移动目标跟踪与定位的位置感知
- 智能家居、工业自动化等的局部控制

由于固线式网络的可靠性和安全性比无线通信系统的高，因此不建议用 WSN 代替有线传感器网络。期望的是共用有线和无线，即混合网络共存。作为有线网络的扩展，WSN 的无线能力任何时候都能为应用增添魅力（Gutierrez 等，2004）。

如果只考虑 WSN 的低成本、低功耗、低数据率和短程通信范围，那么 IEEE

802.15.4 就是设计这类 WSN 最常用的通信标准。ZigBee 和 6LowPAN 协议是两个广泛使用的基于 IEEE 802.15.4 的通信协议。首先，本章以 IEEE 802.15.4 为例介绍 WSN 的基础知识。接着，对 ZigBee 和 6LowPAN 这两个典型的 WSN 进行描述。最后，对 ZigBee 和 6LowPAN 这两种技术进行比较。

2.2 IEEE 802.15.4 协议和无线传感器网络

2.2.1 开放式系统互联模型和无线传感器网络协议栈

由国际标准化组织（International Organisation for Standardisation，ISO）提出的开放式系统互联（Open Systems Interconnection，OSI）七层模型，成为了设计 WSN 协议栈的基础。然而，与由物理层、数据链路层、网络层、传输层、会话层、表示层和应用层组成的七层 OSI 模型不同，WSN 协议栈并没有完全采用 OSI 模型的七层结构。实际上，OSI 模型因层次过多以致过于复杂而难于实施（Aschenbernner，1986）。因此，WSN 协议栈只有五层，如图 2.2 所示。

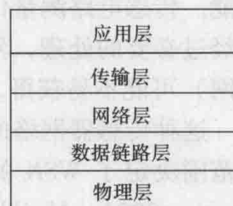


图 2.2　WSN 协议栈

WSN 五层协议栈由物理层、数据链路层、网络层、传输层和应用层组成。协议栈中的每一层都被指定执行一组特定的和其他层不相关的任务。

协议栈的第一层是物理层，负责定义和管理每个设备与通信介质之间的连接，负责频率选择、载波频率生成、信号检测、调制和数据加密。此外，物理层还负责定义连接器的类型，以及与通信介质兼容的电缆。

协议栈的第二层是数据链路层，负责使多个节点能成功访问和共享通信介质，以及媒体访问控制、可靠交付、差错检测和恢复。

协议栈的第三层是网络层，负责网络节点间通信路径的建立，以及沿着这条通信路径成功地传送数据包。如果对路由的需求不一样，那么对路由协议的选择也不相同，但是这种选择会影响通信路径的建立。有些路由协议提供的通信路径有助于为 WSN 提供最佳的服务质量（Quality of Service，QoS），有些节能协议则会使 WSN 获得最佳寿命的路径，而其他的混合协议可以同时满足这两种需求。

第四层是传输层，负责为协议栈的高层提供服务，向端用户之间提供透明的可靠的通信。传输层协议有不同形式，而应用最广泛却截然不同的两个协议是传输控制协议（Transmission Control Protocol，TCP）和用户数据报协议（User Datagram Protocol，UDP）。像 TCP 这样的面向连接的传输层协议能提供可靠的通信服务，具有广泛的差错处理、传输控制和流量控制能力。而如 UDP 这样的无连接的传输层协议提供的是不可靠的通信，仅具有最低程度的差错处理、传输控制和流量控制能力。

大部分 WSN 所采用的第五层，即最后一层，是应用层。应用层和系统用户最近。应用层实现了很多潜在的应用，如远程登录协议（Telnet）、超文本传输协议（Hypertext Fransfer Protocol，HTTP）、文件传输协议（File Fransfer Protocol，FTP）和简单邮件传输协议（Simple Mail Transfer Protocol，SMTP）。就 WSN 而言，其应用层主要是处理信息感知、加密及数据的格式化和存储。此外，应用层还检测下面的协议层是否具有足够的网络资源和服务以满足用户对网络的需求。

2.2.2　IEEE 802.15.4 协议概述

WSN 的嵌入式软件设计需要一些标准以保证网络系统能应用于不同的硬件平台。按照其设计目的的不同，可将当前的标准简单地分为两类：公用标准和专用标准。WSN 生产商使用选定的标准来完成底层开发（无线调制/解调模块、MAC 层协议和网络层协议等）。然后，开发人员从生产商那里购买底层产品，并在其上建立自己的应用。一个单一的标准并不能满足 WSN 的所有功能。实际上，WSN 在概念上没有统一的标准。现有的标准，特别是专用标准，通常只用于指定的应用程序，而可能不适用其他应用程序。例如，如果一个标准为某产品提供一个较长的系统寿命，那么对数据吞吐量的支持可能就会打折。

公用标准相比专用标准对上述问题有更好的平衡性，它的目标是从制造商那里获得尽可能多的支持。为了保证最大的兼容性，开发任意一个公用标准都不得不考虑各种可能的因素。专用标准的开发进程比公用标准快，因为它只需要修改符合自己的目标的标准的内容。然而，正如它的名字一样，专用标准可能不适合公用情况。

IEEE 802.15.4 标准（2003）是为新的低速无线个人局域网（LR-WPAN）标准而设计的。符合 LR-WPAN 标准的应用要求具有低数据吞吐量、低功耗和低的计算能力。它的目标是克服如 Wi-Fi 和蓝牙这样的现有标准存在的一些相关问题。该标准只定义了 LR-WPAN 中的物理（Physical，PHY）层和媒体访问控制（Medium Access Control，MAC）层（IEEE，2003）。IEEE 802.15.4 标准的第 1 版于 2003 年发布。除特别说明，本章所述的 IEEE 802.15.4 标准就是指该版本。

IEEE 802.15.4 标准定义了 PHY 层和 MAC 层规范。该标准不直接提供全面的网络层定义，而只定义了最简单的网络拓扑——星形拓扑和点对点拓扑，这些拓扑可以构成基于该标准的网络基础结构。图 2.3 给出了 IEEE 802.15.4 标准定义的网络架构。

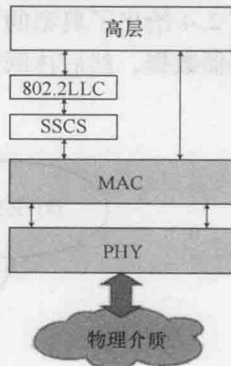


图 2.3　IEEE 802.15.4 标准定义的网络架构（IEEE，2003）

在图 2.3 中，体系结构由两层组成，即物理层和 MAC 层。物理层主要包括无线收发器和相应的底层控制机制。MAC 层为经过物理层的数据传输提供

了定义。特定服务汇聚子层（Service Specific Convergence Sublayer，SSCS）和IEEE 802.2第一类型逻辑链路控制子层为高层访问物理层和MAC层的服务定义了一个标准机制。由于资源有限，WSN应用通常需要使用尽可能简单的协议，这样可以减少系统开销。IEEE 802.15.4的体系结构简单，允许开发者在底层设计直接与数据传输交互的应用软件。许多符合OSI参考模型的传统标准可以提供可靠、充分的服务，但是OSI模型的七层定义使得OSI体系结构复杂而不适用于WSN。

2.2.3 全功能设备和精简功能设备

根据IEEE 802.15.4标准，在IEEE 802.15.4系统中有两种类型的设备，即全功能设备（Full-Function Device，FFD）和精简功能设备（Reduced-Function Device，RFD）。FFD实现了IEEE 802.15.4全部的功能，因此FFD可以作为个人局域网（PAN）协调器（它可以创建和管理整个网络，包括网络建立和从其他设备接受相关请求等）。另外，FFD也可以作为一个协调器（除了不能创建网络，协调器和PAN协调器具有相同功能）或一个普通设备。RFD是实现了协议栈基本功能的设备，即IEEE 802.15.4协议的最小实现。RFD虽然不能用来创建和管理网络，但是可以用来完成极其简单的任务。RFD最通常的用途是将其连接到传感器并定期地将传感器数据发送给网络。在IEEE 802.15.4标准中，FFD可以与其他的FFD和RFD进行通信。高层可以利用这一特点通过路由协议来构建多跳网络。然而，RFD只能与FFD进行通信，因为RFD没有网络管理能力，不适合参与复杂的网络行为，如发送信标信号来同步网络设备。因此，在相同条件下，RFD能比FFD持续的时间更长。一些WSN的应用需要进行长期和独立的监测，因此，频繁地更换分布式传感器节点的电源是不现实的。为了节省能量，RFD更适合实现这样的传感器节点的功能。

在FFD上可以运行比RFD更复杂的应用程序代码，如网络的形成、网络维护、数据包中继、网络设备管理。而对于在RFD上运行的应用程序代码应尽可能简单些。图2.4给出了典型的RFD状态机模型。RFD定期执行传感任务，向控制器报告传感器数据，然后休眠一段时间直到下一轮检测开始时再被唤醒。

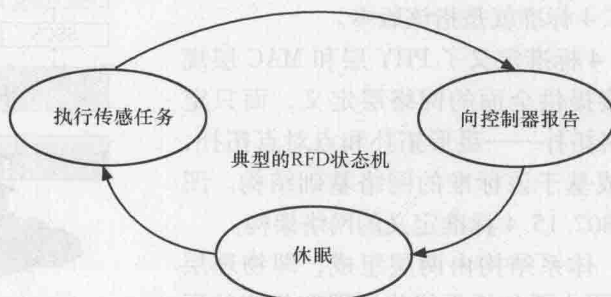


图2.4 典型的RFD状态机模型

2.2.4　IEEE 802.15.4 协议的拓扑结构

IEEE 802.15.4 支持星形、树形、簇树形及网状网络。图 2.5 给出了 IEEE 802.15.4 中的星形和点对点拓扑结构。星形拓扑可以用来形成星形和树形网络，点对点拓扑可以用来形成簇树形网络和网状网络。

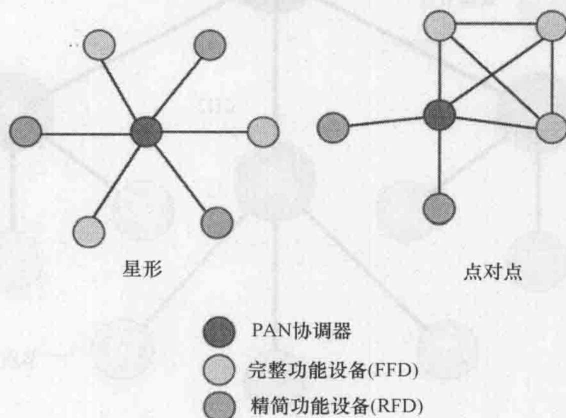


图 2.5　IEEE 802.15.4 中星形和点对点拓扑结构

在星形拓扑中，充当协调器的 FFD 被指定为中央设备，称为 PAN 协调器，负责启动和管理整个网络。其他协调器和网络设备必须与 PAN 协调器相关联，方可加入网络。PAN 协调器控制所有的网络通信。点对点拓扑结构同样需要 PAN 协调器来创建网络启动程序。然而，一个基于点对点拓扑的网络通信并不受到 PAN 协调器的限制。任何一个 FFD 设备都可以与其他 FFD 设备自由通信，只要 FFD 设备在有效通信范围内。任何一个 RFD 设备只能与它的父 FFD 设备通信，而不能与其他 RFD 设备直接通信。RFD 设备和它的父 FFD 设备构成了一个树形拓扑。

簇树形拓扑可以是单簇或多簇的。单簇网络只包含一个簇头（Cluster Head，CH），所有节点一跳连接到 CH，网络拓扑形成星形拓扑。多簇网络包含多个 CH。簇内的每个节点只能与其所在簇的 CH 通信。所有的 CH 构成高一级的子网络，并可直接与它们的 CH 通信。该 CH 可能是连接到外部网络的汇聚节点，或者是所有 CH 的 CH。不同簇中的节点互相不能直接通信，但是可以通过 CH 进行通信。图 2.6 给出了簇树形拓扑结构。该拓扑是层次体系结构，底层为簇网络，高层为 CH 网络。

图 2.7 所示的经由边界节点连接而成的多簇网络，是一个更复杂的簇树形拓扑。图中每个簇用虚线圈注，彼此之间通过边界节点连接。边界节点可以是一个 CH 也可以是一个普通节点。指定设备（Designated Device，DD）需要经过边界节

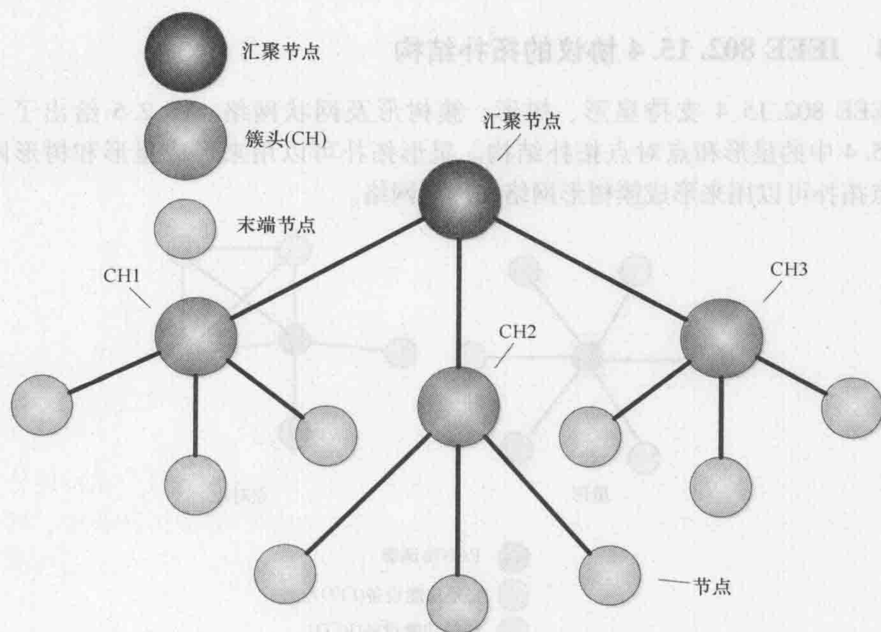


图 2.6 簇树形拓扑结构

点才能与网络连接。DD 与它的边界节点形成簇 0，簇头是 CH0。图 2.7 中，还有另外 4 个簇，簇头分别是 CH1 ~ CH4。CH1 是簇 0 和簇 1 的边界节点，CH3 是簇 1 和簇 3 的簇头。CH1 和 CH3 有两个逻辑地址：一个作为 CH，另一个作为边界节点。与图 2.6 所示的簇树形拓扑不同，图 2.7 所示的为平面网络。

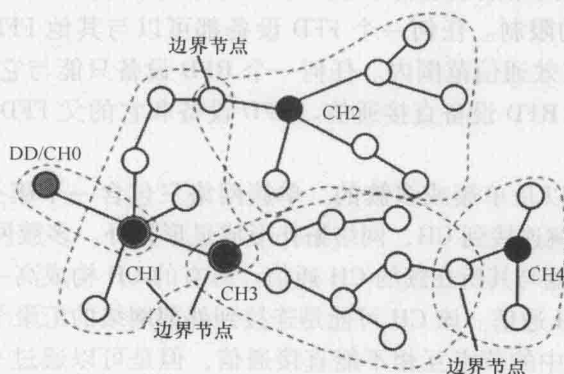


图 2.7 经由边界节点连接而成的多簇网络

2.2.5 IEEE 802.15.4 协议的无线系统多路访问

在各种网络中，无线系统中的无线节点共享一个用于信号传输的公共介质。

IEEE 802.15.4 标准中的多路访问控制（Multiple Access Control，MAC）协议定义了所有节点共享无线介质的方式。这是一种能使总系统性能最大化的方式。无线网络的 MAC 协议大致分为三种：固定分配协议（TDMA 和 FDMA）；随机接入分配协议（CSMA/CA）和按需分配协议（轮询）。这节只讨论无线网络多路访问的最基本概念。

2.2.5.1　跳频/直接序列扩频

跳频扩频（Frequency-Hopping Spead Spectrum，FHSS）技术将 ISM 频段中的科学频段划分为 79 个信道，每个信道带宽为 1MHz。发送端对信息进行划分，并将划分后的信息段发送给不同的信道，这个过程就是跳频。发送端所使用的信道或跳频序列的顺序都是预先定义的，已经通知给了接收端。蓝牙技术就使用 FHSS 技术来进行信息传输。

直接序列扩频（Direct-Sequence Spread Spectrum，DSSS）将每个比特划分为多个比特模式，称为码片。该码片由每个比特和伪随机码进行异或运算获得。然后将异或运算后的结果，即码片发送出去。接收端使用相同的伪随机码对原始数据进行解码。

2.2.5.2　频分多址、时分多址和码分多址

频分多址（Frequency Division Multiple Access，FDMA）把可用频谱划分成多个子频带（即信道），每个子带由一个或多个用户使用。通过 FDMA 的方式，每个用户被分配到一个专用信道，该信道的频带与分配给其他用户的频带不同。用户使用这个专用信道进行信息交换。FDMA 最大的问题是信道彼此之间不能太接近。当发送端使用信道的主频带发射信号时，信道的边带也有能量的输出。因此，为了避免信道间的互扰，需要进行频带分离。

时分多址（Time Division Multiple Access，TDMA）允许用户在时域内共享可用带宽，而不是在频域内。TDMA 将频段划分为多个时隙，每个活动节点被分配一个或多个时隙用于数据传输。

码分多址（Code Division Multiple Access，CDMA）采用一种不同的方法，不是在时域或频域上共享可用的带宽，而是所有节点都处于相同的时间和相同的带宽中。不同用户的传输使用分配给每个用户的唯一代码进行区分。CDMA 常被称为 DSSS。可以通过下面的例子来理解 CDMA：在一个房间里人们使用不同语言进行各种对话；在这种情况下，人们能理解采用自己的语言的对话，而排斥采用其他语言的对话（Nicopolitidis 等，2003）。

2.2.5.3　具有冲突避免的载波侦听多路访问

具有冲突避免的载波侦听多路访问（Carrier-Sense Multiple Access With Collision Avoidance，CSMA/CA）协议是 IEEE 802.11 MAC 层的基础。首先，一个准备传输数据包的 CSMA 节点侦听是否有其他的传输正在进行。如果有其他传输正在进行，节点就等待当前传输完成，然后继续等待一段称为短帧间隔的时段。之后，如

果介质上没有数据流量，节点就开始进行信息传输，否则节点将继续等待直到介质空闲为止。

2.3　使用 IEEE 802.15.4 协议构建无线传感器网络

图 2.8 给出了构建 WSN 的过程。首先是无线信道评估，然后是网络初始化、网络构建公告，接着是以并行方式发生的一些下一步动作。本节用 IEEE 802.15.4 标准中的相关概念介绍建立 WSN 的过程，如图 2.8 所示。

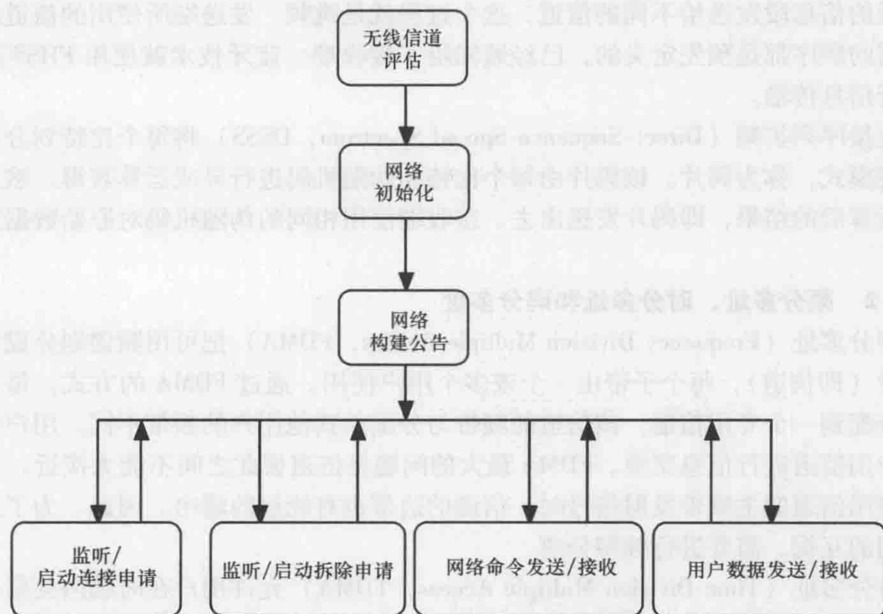


图 2.8　构建 WSN 的过程

2.3.1　无线信道评估

构建无线系统的首要任务是评估所需的传输介质是否可用。评估的细节取决于要设计的无线网络的特点。对于使用跳频的网络，评估的重点是对于所有可用的信道进行分析，然后制定出跳频方案。对于使用 FDMA 访问的网络，评估的重点是寻找最适合网络使用的信道，如具有最少无线活动的空闲信道等。信道评估的另一个重要的问题是，附近与其他使用同一无线频率的系统的共存。由于 WSN 简单、易于部署，多个网络极有可能部署得很近。在信道评估过程中，努力避免与其他网络的冲突是十分关键的。本书第 7 章将介绍互扰抑制的细节。

IEEE 802.15.4 标准规定了关于信道评估的三个功能：能量检测、主动扫描和

被动扫描。下面解释这些术语。

能量检测。能量检测明确定义了系统在指定信道上确定能量大小的能力。任何无线信号的活动都会增加选定信道的能量。因此，使用能量检测可以找出任何潜在的干扰源的位置。

能量检测是评估信道最有效的方式。这种方式可以评估不需要接收的无线信号与 IEEE 802.15.4 收发器是否具有相同的调制和扩频特征。

主动扫描和被动扫描。主动和被动扫描的功能是旨在帮助系统检测附近存在多少个相似的无线网络。在 FFD 协调器启动 IEEE 802.15.4 网络前，FFD 协调器应该至少完成一次主动扫描。FFD 协调器在个人操作空间（Personal Operating Space，POS）范围内发送信标（信标是一种用于同步网络设备的同步信号，通常由网络的 PAN 协调器生成）请求。然后 FFD 协调器将记录接收到的响应，或者叫做信标帧，信标帧包含来自其他现有协调器的网络描述，如图 2.9 所示。通过对接收信息进行比较的结果，当前 FFD 协调器能够确定是否在该区域或指定的信道上启动期望的网络。

被动扫描的过程：如图 2.9 所示，当前的 FFD 接收器在选定的信道上侦听网络信标持续一定的周期。如果其他协调器发送了含有它们网络信息的信标，FFD 接收器使用和主动扫描相同的方法记录和处理该信标。

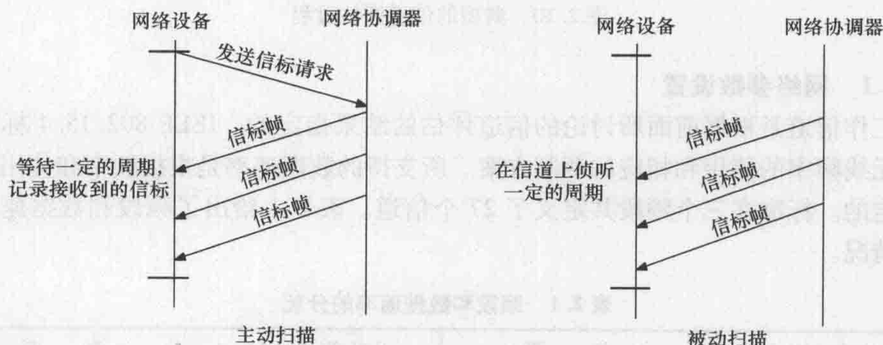


图 2.9　主动/被动扫描

能量检测和主动扫描的功能只能用于 FFD，而被动扫描既可用于 FFD 又可用于 RFD。图 2.10 给出了典型的信道评估过程。其中，在 16 个信道评估中集成了能量检测、主动扫描和被动扫描这些功能。

2.3.2　网络初始化

网络初始化是由 PAN 协调器实现的。网络初始化的内容就是在实际启动一个网络之前指定各种网络参数。这些参数包括工作信道、网络标识符、网络地址分配和 IEEE 802.15.4 网络信标的设置。

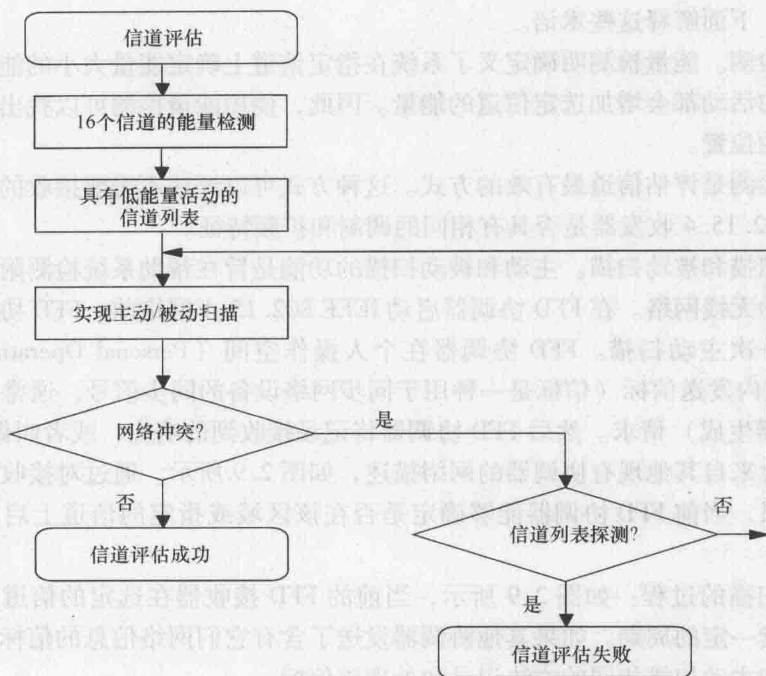


图 2.10 典型的信道评估过程

2.3.2.1 网络参数设置

工作信道是根据前面所讨论的信道评估的结果指定的。IEEE 802.15.4 标准定义了无线频率的使用和相应的调制方案。所支持的数据速率是根据频率和使用的调制指定的。标准在三个频段共定义了 27 个信道。表 2.1 给出了频段和数据速率的分配情况。

表 2.1 频段和数据速率的分配

频段/MHz	信 道	比特率（kbit/s）	调 制
868 ~ 868.6	0	20	BPSK
902 ~ 928	1 ~ 10	40	BPSK
2400 ~ 2483.5	11 ~ 26	250	O-QPSK

因为 IEEE 802.15.4 标准不支持动态数据速率变化或跳频，必须提前指定频率使用方案。另一个问题是频段选择。频段选择需要遵守无线电规定及将要部署的系统的本地规定。

确定了工作信道之后，系统应该选择网络标识符。通过该网络标识符其他设备可以识别网络。对于网络系统，IEEE 802.15.4 标准支持 16 位长的网络标识符（即 PAN ID）用于标记每个网络。PAN ID 的选择必须是唯一的，不能和其无线范

围内的其他网络的网络标识一样。因此，主动或被动扫描对指定的网络可以提供有用信息。

IEEE 802.15.4 标准定义了两种基本的通信地址模式，即扩展地址模式和短地址模式。扩展地址模式使用的64位长的数字在生产设备时就被固化到了固件里。64位地址可以确保设备的唯一性。扩展地址模式的缺点是将降低数据包有效载荷的大小。短地址模式使用16位长的数字。PAN协调器启动网络时负责产生的16位网络地址。例如，一个PAN协调器可以设置自己的网络地址为0x0000。随后加入该网络的设备都可以通过PAN协调器地址加1的方式得到一个16位的网络地址，如0x0001、0x0002等。短地址模式的长度决定了网络容量理论上不能超过65535（即2^{16}）。IEEE 802.15.4网络中使用的短地址模式可以增加数据包有效载荷的大小，但短地址模式必须与PAN ID关联。否则，短地址的唯一性不能得到保证。IEEE 802.15.4标准没有提供默认的短地址分配方案，网络开发人员可以基于应用需求设计出一个合适的方案。

2.3.2.2　超帧结构

IEEE 802.15.4 标准里的低功耗的特点是通过低占空比的设定来实现的。无线系统中消耗功率最大的组件是收发器。IEEE 802.15.4 收发器典型的工作电流约为20～30mA。如果收发器一直保持工作状态，特别是收发器由电池供电时，这将是很大的能耗。IEEE 802.15.4 标准定义了超帧结构，以使系统能够降低对收发器的使用，同时使网络仍然起作用。

超帧结构是一个由网络信标界定的时间周期。一收到信标，网络设备的收发器就启动同步功能，并开始在超帧范围内执行预定的任务。超帧结构指定了收发器处于活动状态的周期。一个活跃周期结束后，收发器停止工作，在接下来的不活动周期内保持休眠状态直到下一个信标的到来。同步机制意味着系统在不中断通信的情况下有节能的可能性。为了保证设备与相同的源设备同步，发送网络信标的PAN协调器在网络的整个生命周期内需要保持供电。图2.11给出了超帧结构，其英文缩写和中文含义见表2.2所示。

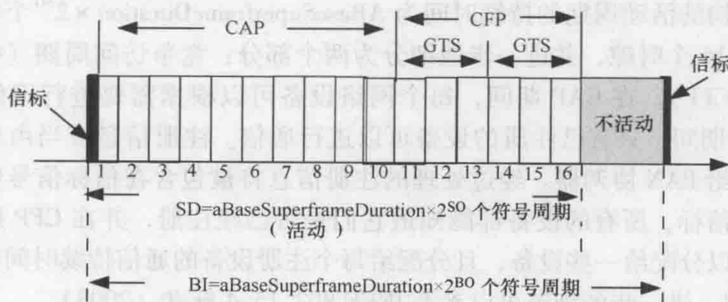


图2.11　超帧结构

表 2.2 超帧结构中技术术语的英文缩写及中文含义

英文缩写	中文含义（全拼）
CAP	竞争访问周期（Contention Access Period）
CFP	无竞争周期（Contention Free Period）
GTS	保证时隙（Guaranteed Time Slot）
SD	超帧持续时间（Superframe Duration）
SO	超帧阶数（Superframe Order）
BI	信标间隔（Beacon Interval）
BO	信标阶数（Beacon Order）

如图 2.11 所示，超帧结构包括两个主要部分：活动周期和不活动周期。活动周期的长度可表示为超帧持续时间（SD），可由下式

$SD = aBaseSuperframeDuration \times 2^{SO}$ 个符号周期计算得到：

式中，超帧阶数（SO）的范围为 0 ~ 15；aBaseSuperframeDuration 由时隙数（大多数情况下为 16）与基本时隙持续时间（大多数情况下为 60）的乘积计算得到。超帧结构整个持续时间叫做信标间隔（BI），由活动周期和不活动周期构成，且可由下式

$BI = aBaseSuperframeDuration \times 2^{BO}$ 个符号周期计算得到：

式中，信标阶数（BO）的范围为 0 ~ 15。SO 和 BO 值的关系为 $0 \leqslant SO \leqslant BO \leqslant 14$。这是因为如果 $BO = SO = 15$，那么 SO 的值可以忽略且超帧将不存在，此时收发器将处于无节能的持续工作状态。

如果 $0 \leqslant SO = BO \leqslant 14$，那么 BI 的长度将等于活动周期，所以不活动周期将不存在。如果 $0 < SO < BO \leqslant 14$，SD 和 BI 之间的差就是不活动周期，在此期间所有的网络通信保持休眠直到下一个信标的到来。

一收到信标，网络设备就可以开始实现所设计的通信。如果 $SO < BO$，通信必须在活动周期结束前停止；或者如果 $SO = BO$，通信必须在超帧周期结束前停止。

超帧结构的活动周期的持续时间为 $ABaseSuperframeDuration \times 2^{SO}$ 个符号周期且被平均分为 16 个时隙，并进一步地细分为两个部分：竞争访问周期（CAP）和无竞争周期（CFP）。在 CAP 期间，每个网络设备可以根据需要进行网络通信。然而，在 CFP 期间，只有已注册的设备可以进行通信。注册信息应当由相应的网络设备提前交给 PAN 协调器。经过处理的注册信息将被包含在信标信号中。通过检查接收到的信标，所有的设备都能知道它们是否已经注册，并在 CFP 期间进行通信。CFP 可以分配给一些设备，且分配给每个注册设备的通信持续时间由保证时隙（GTS）控制。进一步的细节可以参考 IEEE 802.15.4 标准（2003）。

一旦选定了 BO 和 SO，就可以计算出占空比。例如，对于 2.4GHz 频段 16 个信道中的一个信道，如果 BO 和 SO 分别设定为 3 和 2，BI 和 SD 可以由下面两式的

计算得到：

$$\begin{aligned}BI &= aBaseSuperDuration \times 2^{BO}\text{个符号周期}\\ &= numberOfSlots \times baseSlotDuration \times 2^{BO}\text{个符号周期}\\ &= (16 \times 60 \times 2^{3} \times 16)\mu m = 122.88ms\end{aligned} \tag{2.1}$$

$$\begin{aligned}SD &= aBaseSuperDuration \times 2^{SO}\text{个符号周期}\\ &= (960 \times 2^{2} \times 16)\mu s = 61.44ms\end{aligned} \tag{2.2}$$

PAN 协调器大约每秒产生约 8 个信标（1000/122.88≈8）。在每个 BI 期间，网络设备的收发器大约工作 61.44ms，然后在剩余的时间保持休眠。因此，占空比约为 50%（61.44/122.88 = 0.5），简要地说，大约节省了 50% 的能耗。

使收发器在“开或闭”模式下工作虽然可以节省能耗，但是可能会造成两个问题：第一，系统可能在给定的时间内不能完成一次完整的数据传输和接收；第二，系统的响应可能会延迟。对于第一种情况，需要计算用于传送单个数据包的时间。一个完整的 IEEE 802.15.4 数据包为 133 字节（IEEE 2003）。使用给定的数据速率，如 2.4GHz 频段的 250kbit/s，发送一个 IEEE 802.15.4 的数据包所需的时间最大为 4.256ms，即 $[(133 \times 8)/(250 \times 10^{3})]$ s。如图 2.11 所示，超帧的活动周期应该足够长以在一个信标间隔内能完成一次数据传输。

为了解决在数据传输中由“开关”模式引起的响应延迟，应设置一个恰当的占空比（即 BI 和 SD），因为设置一个低占空比会延缓系统响应。表 2.3 给出了占空比为 50% 时 BO 和 SO 的设置情况，BO = SO = 0 的情况除外。

表 2.3 占空比为 50% 时 BO 和 SO 的设定情况

BO	SO	BI/ms	SD/ms	不活动周期/ms
0	0	15.36	15.36	0
1	0	30.72	15.36	15.36
2	1	61.44	30.72	30.72
3	2	122.88	61.44	61.44
4	3	245.76	122.88	122.88
5	4	491.52	245.76	245.76
6	5	983.04	491.52	491.52
7	6	1966.08	983.04	983.04
8	7	3932.16	1966.08	1966.08
9	8	7864.32	3932.16	3932.16
10	9	15728.64	7864.32	7864.32

表 2.3 中，SO 比 BO 小 1（BO = SO = 0 的情况除外）。因此，占空比稳定在 50%。如标准定义的，当没有可用的无线通信时，网络将在不活动周期持续的时间

内保持休眠。BO 为 1 ~ 6 时，BI 小于 1s，这对大多数应用来说这是可以接受的。而当 BO 为 7 ~ 10 时，出现相当大的延迟，因为不活动周期的持续时间为 1983.04 ~ 7864.32ms。增加 SO 能降低系统响应延迟，降低 BI，即增加占空比。然而，高占空比又会增加功耗、不节能。

实现系统性能和功率之间的平衡虽然是任何具有电源限制应用的挑战，但是应用的特定解决方案是可以实现的。如果 BO 和 SO 都被设置为 15，就不会存在节能问题，因为超帧结构不存在。

2.3.3 网络构建公告

在对网络参数初始化后，PAN 协调器就可以公告网络构建成功了。用于公告网络构建的实际过程是由所使用的网络协议确定的。公告的目的是向其他设备指明当前无线系统的存在。实现这个目的有两种方式：主动公告或收到请求后的被动应答。有些无线协议定期地使用信标信号来同步网络操作。这种类型的网络叫做信标使能网络。信标还向新启动的设备报告当前无线系统的一些特征，如工作通道、频段、物理位置等。如果协议不支持信标信号的定期发送，这种类型的网络叫做非信标使能网络。PAN 协调器将对工作信道保持监听，并对执行无线信道评估的设备发出的任何有效请求做出响应。

对于一个信标使能网络，在网络构建公告后，根据设置的 SO 和 BO 的值，定期地发送信标信号。在网络的整个工作周期中，PAN 协调器应确保信标传输的持续性，以便使其能够被一些被动扫描设备检测到，同时也能够响应其他设备发起的主动扫描。

2.3.4 监听/启动连接申请

在成功地初始化 IEEE 802.15.4 网络后，PAN 协调器就成为了主要的网络管理者。除非 PAN 协调器的收发器忙于数据传输，否则它应该一直监听选定的工作信道，以便执行网络管理的职责。

任何希望加入网络的设备应实现三个基本步骤：启动主动扫描（仅 FFD）或被动扫描以便找到期望的 PAN 协调器，与可用的网络信标同步（0 < SO < BO < 14），以及通过向找到的 PAN 协调器发出相关请求来申请加入网络。一旦接收到该连接申请，PAN 协调器按照所设计的过程来核对该申请。如果申请被批准，PAN 协调器可以决定如何向该设备分配网络地址，然后向该设备返回一个包含网络信息（如网络地址）和批准决定的响应。如果连接申请被拒绝，PAN 协调器应返回相应的反馈信息。一接收到来自 PAN 协调器的响应，网络设备就可以使用分配到的地址实现网络通信，或调用预定算法处理“连接失败”响应。

2.3.5 监听/启动移除申请

处理移除申请是处理连接申请的逆过程。PAN 协调器可以从接收设备列表中

删除该设备的地址，并向该设备通知移除决定。或者，当收到网络设备的移除申请时，PAN 协调器就执行上面的过程。一收到 PAN 协调器的通知，该设备要保证移除申请是被允许的。

2.3.6　网络命令发送/接收

网络命令的发送和接收主要用于网络管理。网络命令通常不需要用户知道，也不需要用户干预。但是，有时需要用户干预的命令直到获得用户的指令才会执行。因此，在系统设计中，必须有处理这类应用的处理模块。例如，当一个网络设备注意到附近有另一个 IEEE 802.15.4 的网络在运行并使用相同的网络 ID，该网络设备向 PAN 协调器发送一个冲突通知命令。然后，PAN 协调器启动主动扫描，并通过广播协调调整命令确定一个新的 PAN ID。在这种情况下，新的 PAN ID 的选择就需要由用户干预来完成。另一个例子是，一个网络系统对采用的新设备开始增加安全级别时，这样的设备申请细节都需要由高层管理系统进行审查，随后将进行网络命令的发送和接收。

2.3.7　数据发送和接收

在 IEEE 802.15.4 标准中，根据信标的使用可以对数据的发送和接收进行分类。图 2.12 给出了 IEEE 802.15.4 标准中通信的方法。图 2.12 中有两个通信方向：从协调器到网络设备和从网络设备到协调器。

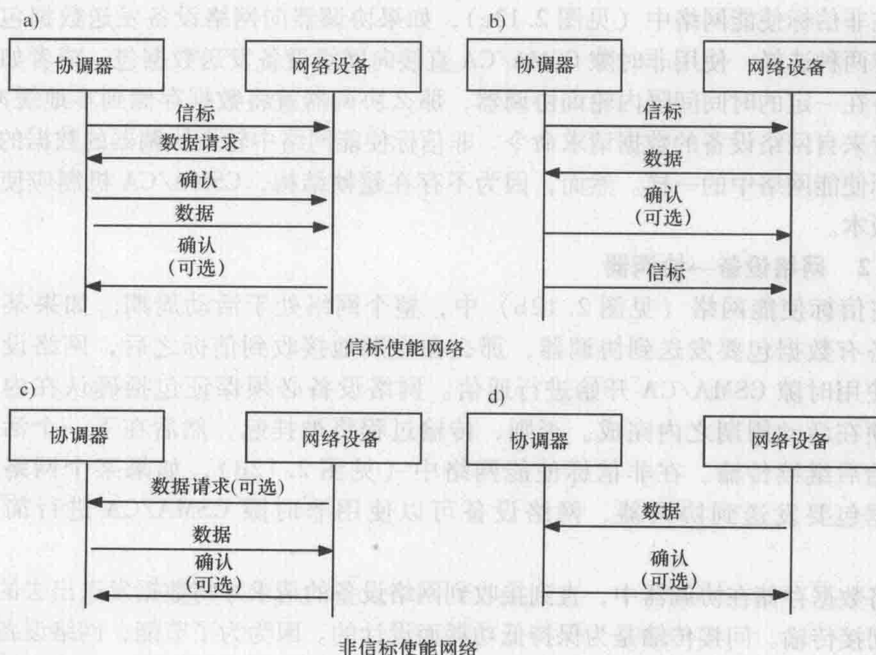


图 2.12　IEEE 802.15.4 标准中通信的方法

2.3.7.1 协调器→网络设备

如图2.12a所示，在信标使能网络中，当协调器有数据包要发送到网络设备时，协调器将数据存储在本地缓存区，并将该数据包信息（即目的地址）放到信标帧中的“地址挂起列表”。网络设备一收到信标帧，就会知道协调器里是否有挂起的数据包。网络设备有两种选择继续进行通信：如果网络设备的macAutoRequest，即MAC响应模式指示设置为TRUE，则网络设备使用时隙CSMA/CA向协调器自动发送请求命令来请求挂起的数据。如果macAutoRequest设置为FALSE，则栈就把“信标通知”原语上交到应用层，并让应用层决定是否有必要发送数据请求命令。一收到数据请求命令，协调器首先确定向网络设备发送确认信号的方式。如果协调器检查本地缓冲区，并确定发往网络设备的挂起的数据包还存在，那么就在macAckWaitDuration（即预定义持续时间期间）发送确认。如果在规定时间内不能完成确认的发送，协调器应发送数据挂起域（即挂起状态指示）设置为1的确认。在发送确认后，如果在前面的确认帧中数据挂起域设置为1，则协调器应向网络设备发送数据包。如果没有挂起的数据，则数据有效载荷的长度为0。一收到确认，如果确认数据包的数据挂起域为1，那么，网络设备就使接收器持续aMaxFrameResponseTime最大持续时间。网络设备可能需要回送一个确认，以指示成功接收。从协调器到网络设备的数据帧发送应采用时隙CSMA/CA机制。

在非信标使能网络中（见图2.12c），如果协调器向网络设备发送数据包，协调器有两种选择：使用非时隙CSMA/CA直接向网络设备发送数据包；或者如果网络设备在一定的时间间隔内轮询协调器，那么协调器就将数据存储到本地缓冲区，并等待来自网络设备的数据请求命令。非信标使能网络中轮询协调器的数据的过程和信标使能网络中的一样。然而，因为不存在超帧结构，CSMA/CA机制应使用非时隙版本。

2.3.7.2 网络设备→协调器

在信标使能网络（见图2.12b）中，整个网络处于活动周期。如果某个网络设备有数据包要发送到协调器，那么在定期地接收到信标之后，网络设备就可以使用时隙CSMA/CA开始进行通信。网络设备必须保证包括确认在内的传输必须在活动周期之内完成。否则，传输过程将被挂起，然后在下一个活动周期开始后继续传输。在非信标使能网络中（见图2.12d），如果某个网络设备有数据包要发送到协调器，网络设备可以使用非时隙CSMA/CA进行简单的通信。

将数据存储在协调器中，直到接收到网络设备的请求才将数据发送出去的方法叫做间接传输。间接传输是为保持低功耗而设计的。因为为了节能，网络设备通常处于睡眠状态，且无线接收器处于关闭状态。将数据存储在协调器中可以使网络设备获取信息更方便，而不需要接收器一直保持开启状态。当有一个时隙可用时，网

络设备就可以发送数据请求命令。

2.3.8 时隙和非时隙具有冲突避免的载波侦听多路访问

如上一节中提到的，信标使能网络和非信标使能网络在数据传输时都使用 CSMA/CA。CSMA/CA 有两个版本可以使用：用于信标使能接入的时隙 CSMA/CA 和用于非信标使能接入的非时隙 CSMA/CA。“时隙”的概念只在信标使能网络中使用。图 2.13 给出了在 BO = SO = 0 的超帧结构中的时隙和退避周期。

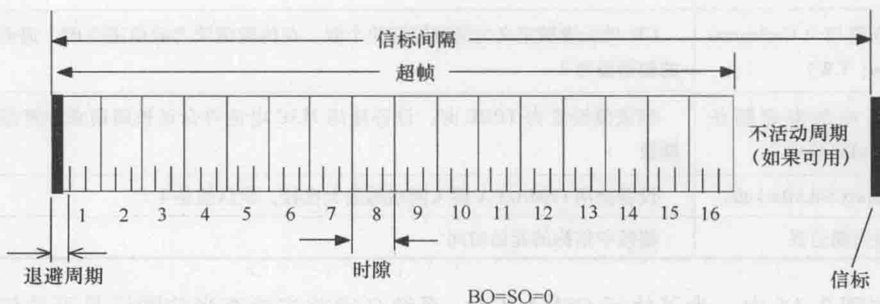


图 2.13 在 BO = SO = 0 的超帧结构中的时隙和退避周期

如图 2.13 所示，超帧结构被分成 16 等份，其中每个等份叫做“时隙”。用来在每个时隙中找到恰当时间点的基本单元叫做“退避周期”，由符号 aUnitBackoffPeriod 表示，是设备再次接入网络必须等待的时间。因为超帧中的时隙数设置为 16，所以根据式（2.2），单个时隙的持续时间为

$$T_{\text{SuperframeSlot}} = \frac{\text{SD}}{16} = \frac{(60\times16\times2^{\text{SO}})\text{个符号周期}}{16} = (60\times2^{\text{SO}})\text{个符号周期} \quad (2.3)$$

单个退避周期的持续时间定义为

$$T_{\text{Backoff_Period}} = \text{aUnitBackoffPeriod} = 20\text{ 个符号周期}$$

单个时隙内的退避周期数 $N_{\text{Backoff_Period}}$ 为定义为

$$N_{\text{Backoff_Period}} = \frac{T_{\text{SuperframeSlot}}}{T_{\text{Backoff_Period}}} = \frac{(60\times2^{\text{SO}})\text{个符号周期}}{20\text{ 个符号周期}} = 3\times2^{\text{SO}} \quad (2.4)$$

图 2.13 中，每个时隙的退避周期数是 3，其中 SO = 0。

表 2.4 给出了 CSMA/CA 操作相关技术术语。图 2.14 给出了 IEEE 802.15.4 标准中时隙的和非时隙 CSMA/CA 操作的流程图。

表 2.4 CSMA/CA 操作相关技术术语

术 语	含 义
退避周期单位	设备再次访问网络前必须等待的时间
退避指数（Backoff Exponent，BE）	在信道忙时，试图发送一个数据包之后，再次尝试重传之前必须等待的时间
macMaxBE	最大退避指数，总是 5
macMinBE	最小退避指数，总是 3
退避数（Number of Backoffs，NB）	试图使用 CSMA/CA 接入网络的次数，初始值为 0
竞争窗口（Contention Window，CW）	CW 的长度被定义为退避周期的个数，在传输继续之前信道空闲，退避周期的初始值为 2
MAC 电池寿命延长（macBattLifeExt）	当该值设置为 TRUE 时，设备使用 MAC 电池寿命延长周期来计算退避周期数
macMaxCSMABackoffs	设备使用 CSMA/CA 接入网络的最大次数，默认值是 4
退避周期边界	超帧中信标的起始时间

在图 2.14 中，为了执行 CSMA/CA，系统必须首先检查当前网络是否是信标使能网络。如果是就使用左侧的时隙 CSMA/CA；否则，就使用右侧的非时隙 CSMA/CA。

在时隙 CSMA/CA 中，应对三个参数 NB，CW 和 BE 应在执行前进行初始化。NB 的初始值设置为 0。CW 的初始值设置为 2，且当信道忙时重新设置为 2。BE 为退避指数，指明设备在试图接入信道前应执行多少个退避周期。如果参数 macBattLifeExt 设置为 FALSE，则 BE 应等于 macMinBE 值。否则，BE 应初始化为 2 和 macMinBE 值两者中较小的那个。在完成参数初始化后，系统将确定下一个可用的退避周期边界（点 1）。然后系统将延迟一定的退避周期，其数值在 0 ~ $(2^{BE}-1)$ 随机选择（点 2）。当延迟结束时，系统将在下一个可用的退避周期边界上执行 CCA。一个由 IEEE 802.15.4 标准定义的重要规则是，在第一次试图随机延迟之前，MAC 层应判定延迟是否可以在 CAP 结束之前完成。如果不能完成，系统将在 CAP 结束时暂停计数，并在下一个超帧开始时继续。如果能完成，系统应当使用退避延迟。当退避延迟结束后，系统将再次评估以确定剩余部分操作，包括两个 CCA 分析、数据帧传输和接收可能的确认，能否在 CAP 结束之前完成。如果 MAC 层能够处理这些操作，系统应马上就开始执行 CCA（点 3）。如果不能，则系统应停止并等待下一个超帧，然后反复进行评估。

如果评定信道为忙，CW 将被重置为 2，NB 的值将增加 1。BE 的值为 BE + 1 和 macMaxBE 这两者中较小的一个。如果 NB 的值大于 macMaxCSMABackoffs，就宣告当前尝试失败。如果不大于，就跳转到点 2，如果评定信道为空闲，系统就将

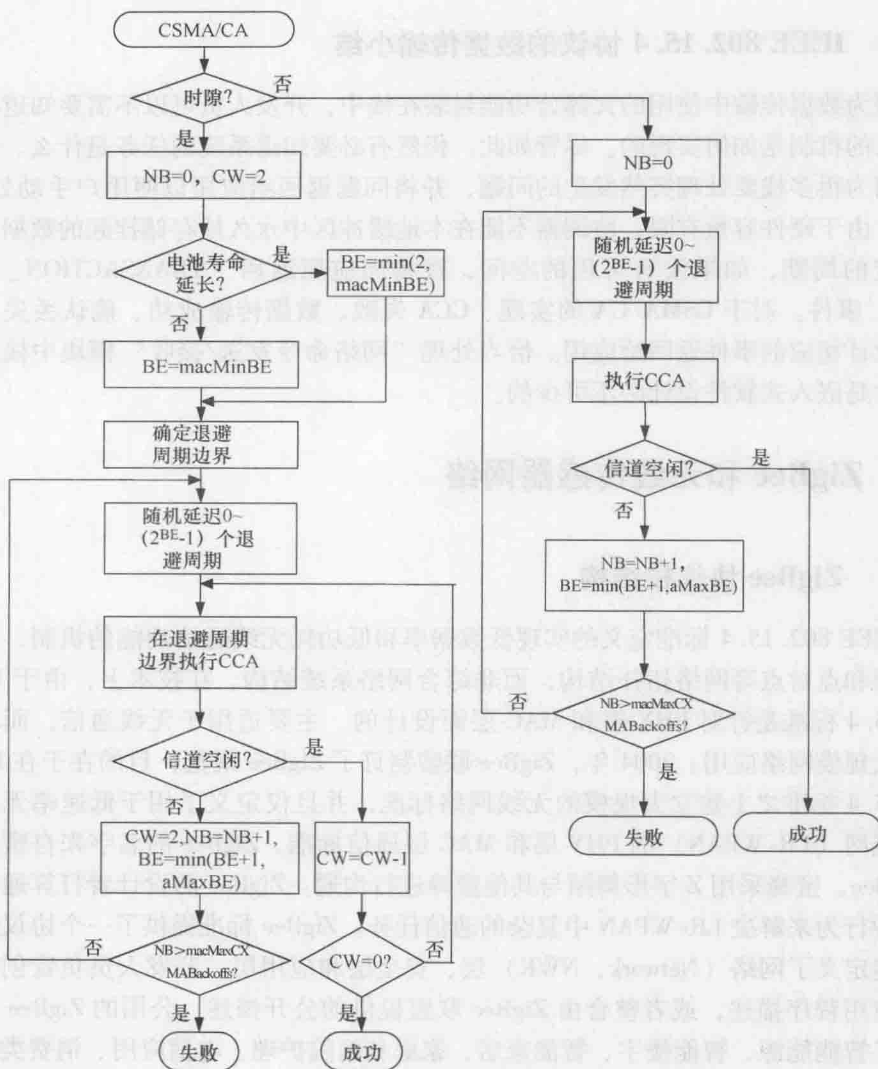


图 2.14　IEEE 802.15.4 标准中时隙和非时隙 CSMA/CA 操作的流程图

CW 值减 1。如果 CW 值不等于 0，系统就跳转到点 3。否则，MAC 层就在下一个可用的退避周期边界开始数据传输。

在非时隙系统（即非信标使能网络），需要对参数 NB 和 BE 进行初始化。NB 设置为 0，BE 设置为 macMinBE。初始化后，系统应该延迟一定的退避周期，其值在 0 ~（$2^{BE}-1$）随机选择（点 4）。在延迟之后，MAC 层执行 CCA（点 5）。如果评定信道为忙，将 NB 的值加 1，BE 的值为 BE + 1 和 macMaxBE 两者中较小的一个。如果 NB 大于 macMaxCSMABackoffs，宣告当前尝试失败。如果不大于，就跳转到点 4。如果评定信道空闲，MAC 层就立即开始数据传输。

2.3.9 IEEE 802.15.4 协议的数据传输小结

因为数据传输中使用的大部分功能封装在栈中，开发人员可以不需要知道标准中定义的机制是如何实现的。尽管如此，仍然有必要知道系统的任务是什么。特别地，因为很多栈要处理突然发生的问题，并将问题返回给应用以便用户手动处理。例如，由于硬件容量有限，协调器不能在本地缓冲区中永久地存储挂起的数据。经过一定的周期，如果没有可用的空间，栈将向应用返回“TRANSACTION_ EX-IRED”事件。对于 CSMA/CA 的实现、CCA 失败、数据传输成功、确认丢失，都需要设计相应的事件返回给应用。恰当处理“网络命令发送/接收”模块中栈的返回事件是嵌入式软件设计必不可少的。

2.4 ZigBee 和无线传感器网络

2.4.1 ZigBee 协议栈结构

IEEE 802.15.4 标准定义的实现低数据率和低功耗无线通信功能的机制，只支持星形和点对点等网络拓扑结构，而非综合网络系统结构。在技术上，由于 IEEE 802.15.4 标准是针对 PHY 层和 MAC 层而设计的，主要适用于无线通信，而不是针对大规模网络应用。2004 年，ZigBee 联盟制订了 ZigBee 规范，目的在于在 IEEE 802.15.4 标准之上建立大规模的无线网络标准，并且仅定义了用于低速率无线个人区域网（LR-WPAN）的 PHY 层和 MAC 层通信标准。ZigBee 的名字来自蜜蜂的英文 Bee。蜜蜂采用 Z 字形舞蹈与其他蜜蜂进行沟通。ZigBee 的设计者打算通过模仿这种行为来解决 LR-WPAN 中复杂的通信任务。ZigBee 标准提供了一个协议栈分别描述定义了网络（Network，NWK）层、安全层和应用层。开发人员负责创建自己的应用程序描述，或者整合由 ZigBee 联盟提供的公开描述。公用的 ZigBee 描述包含了智能能源、智能楼宇、智能家居、家庭和医院护理、电信应用、消费类电子产品控制，以及工业过程监视与控制（Elahi 和 Gschwender，2009）。ZigBee 标准的最新版本是 2007 年发布的 ZigBee PRO。图 2.15 给出了 IEEE 802.15.4 标准和 ZigBee 协议栈的关系。

ZigBee 标准的特点主要是低数据率、低成本、低复杂度、低功耗及易于实现。表 2.5 给出了 ZigBee、Wi-Fi 及蓝牙（IEEE 802.15.1）的比较。从表 2.5 所示可以知道，Wi-Fi、蓝牙和 ZigBee 使用工业、科研和医疗应用（Industrial、Scientific research and Medical applications，ISM）频段。该频段免许可证且传输功率小于 1W。图 2.16 给出了由美国联邦通信委员会（Federal Communication Committee，FCC）提出的 ISM 频段的频率分配情况。ZigBee 可以在 I-频段、S-频段或 M-频段使用，而 Wi-Fi 和蓝牙只能在 S-频段使用。



图 2.15　IEEE 802.15.4 标准和 ZigBee 协议栈的关系

表 2.5　ZigBee、Wi-Fi 及蓝牙的比较（Elahi 和 Gschwender，2009）

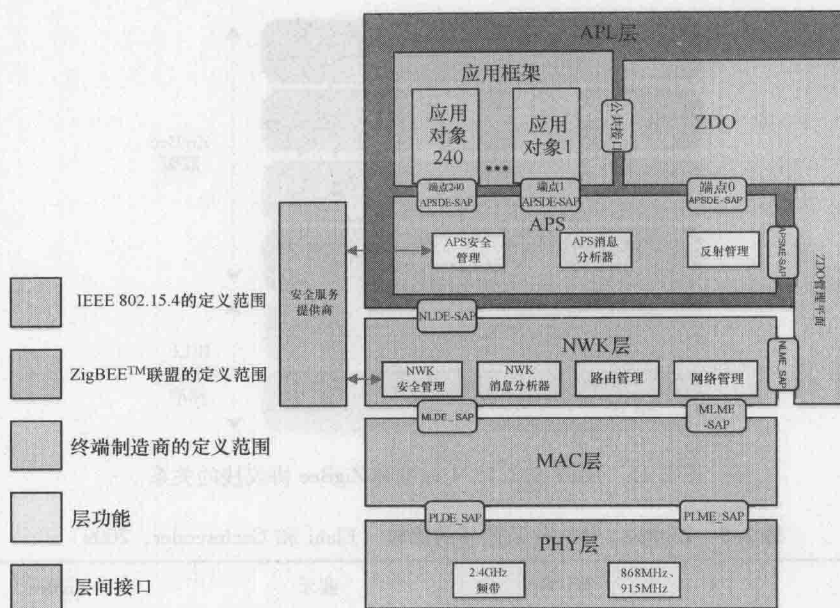
	Wi-Fi (IEEE 802.11)	蓝牙 (IEEE 802.15.1)	ZigBee (IEEE 802.15.4)
应用	无线局域网	替代有线	控制与监视
频段	2.4GHz	2.4GHz	2.4GHz、868MHz 和 915MHz
电池寿命/天	0.1 ~ 5	1 ~ 7	100 ~ 700
每个网络的节点数	30	7	65000
带宽	2 ~ 100Mbit/s	1Mbit/s	20 ~ 250kbit/s
范围/m	1 ~ 100	1 ~ 10	1 ~ 75
拓扑结构	树形	树形	星形、树形、 簇树形、网状
待机电流/A	20×10^{-3}	200×10^{-6}	3×10^{-6}
存储器/KB	100	100	32 ~ 60

902MHz　928MHz　2.4GHz　2.48GHz　5.725GHz　5.85GHz

工业频段 (I-频段)		科研频段 (S-频段)		医疗频段 (M-频段)

图 2.16　美国联邦通信委员会提出的 ISM 频段的频率分配情况

图 2.17 所示的 ZigBee 协议栈结构由三部分组成，如下所示：



APSME-SAP:应用支持子层管理实体-服务访问点,Application Support Sublayer Management Entity-Service Access Point
NLDE_SAP:网络层数据实体-服务访问点,Network Layer Data Entity-Service Access Point
NLME_SAP:网络层管理实体-服务访问点,Network Layer Management Entity-Service Access Point
MLDE_SAP,媒体访问控制层数据实体-服务访问点,MAC Layer Data Entity-Service Access Point
MLME_SAP,媒体访问控制层管理实体-服务访问点,MAC Layer Management Entity-service Access Point
PLDE_SAP,物理层数据实体-服务访问点,PHY Layer Data Entity-Service Access Point
PLME_SAP,物理层管理实体-服务访问点,PHY Layer Management Entity-Service Access Point

图 2.17　ZigBee 的协议栈结构（2004）

● IEEE 802.15.4 标准，定义 MAC 层和 PHY 层。

● ZigBee 部分，它包含 NWK 层、应用支持子层（Application Support Sublayer，APS）、安全服务管理和 ZigBee 设备对象（ZigBee Device Object，ZDO）部分。端点是一个应用对象，最多可以支持 240 个单独的应用对象。端点定义了到 APS 的输入和输出。ZDO 负责应用对象的控制和管理。

● ZigBee 的应用部分，开发人员可以使用 ZigBee 应用描述或开发自己的应用描述。

在 ZigBee 规范中，网络设备被分为三种类型：ZigBee 协调器、ZigBee 路由器及 ZigBee 终端设备。ZigBee 协调器是一种基于 IEEE 802.15.4 的 PAN 协调器，它是全功能设备。任何一个 ZigBee 网络应该有且只有一个 ZigBee 协调器。ZigBee 协调器具有为新创建的网络选择可用信道和相应的网络标识符（16 位长度）的功能。作为启动 ZigBee 网络的第一个设备，ZigBee 协调器负责新设备的采用和网络地址的分配。

ZigBee 路由器是一种基于 IEEE 802.15.4 的全功能设备。ZigBee 路由器提供了选择加入现有 ZigBee 网络的功能，以及通过采用超出 ZigBee 协调器通信范围的新设备来扩展 ZigBee 网络。此外，通过实现所设计的路由协议，ZigBee 路由器构建了 ZigBee 网络的主干网络。

ZigBee 终端设备是基于 IEEE 802.15.4 的全功能设备或精简功能设备。ZigBee 终端设备通常部署在网络的末端来执行传感任务。精简功能设备更适合这样的应用，因为它们更节能。

2.4.2　ZigBee 拓扑结构

2.4.2.1　ZigBee 拓扑结构

ZigBee 位于 IEEE 802.15.4 之上，并使用 IEEE 802.15.4 规范作为自己的 MAC 层和 PHY 层规范。ZigBee 网络通过扩展点对点拓扑结构来支持星形、树形和网状拓扑结构，如图 2.18 所示。

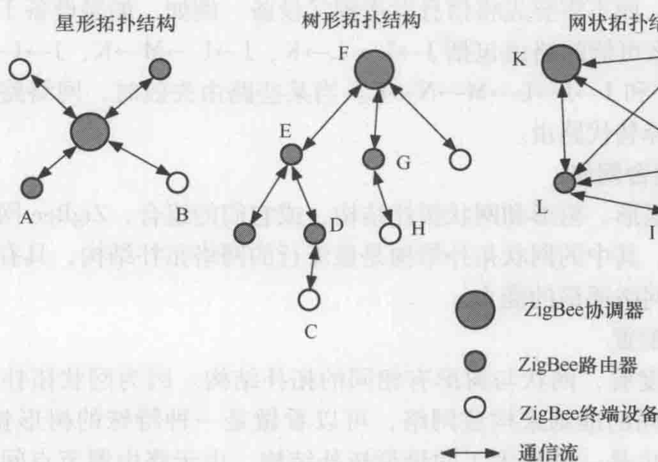


图 2.18　ZigBee 规范中的 3 种网络拓扑结构

如图 2.18 所示，星形拓扑结构是最容易实现的拓扑。ZigBee 协调器是网络的中心节点，ZigBee 路由器和 ZigBee 终端设备等其他 ZigBee 设备需要连接到 ZigBee 协调器来构成网络。由于 ZigBee 协调器的限制，星形拓扑结构不适合大规模的应用。因为所有的设备都必须通过 ZigBee 协调器加入网络，而超出协调器无线范围的设备就不能加入网络了。星形拓扑结构主要缺点是中心节点（ZigBee 协调器）出现故障后将影响整个网络。在星形网络中的设备彼此不能直接通信。例如，在图 2.18 所示的星形拓扑结构中，如果设备 A 想向设备 B 发送一条信息，则该信息将首先发送到 ZigBee 协调器，然后再转发到目的 B 中。

与星形拓扑结构相比，树形拓扑结构更具灵活性，其部署不受协调器限制，并

且可以通过 ZigBee 路由器采用子设备来扩展范围。树形网络的构成准则：终端设备通过路由器设备加入树形网络，一个路由器设备通过另一个路由器设备（ZigBee 协调器也可以作为一个路由器设备）加入树形网络。路由器设备可以采用终端设备或其他的路由器设备作为其子设备，子设备也称为“孩子”。而终端设备不能有“孩子”。因此，终端设备不能是父设备。树形网络的通信必须遵守这些规则。例如，在图 2. 18 所示的树形拓扑结构中，若设备 C 欲将信息发送到设备 H，信息应先通过设备 D 和 E 发送回设备 F，然后设备 F 通过设备 G 将信息发送到设备 H。信息传送准则：信息必须从源节点沿着树向上传到最近的与目标节点共同的祖节点，然后沿着树下传至目的节点（ZigBee，2004）。其缺点是，路径上的任何一个设备出故障后没有可用的替代路由。但是，实现路由协议相当容易，因为每个设备只需维护一个树表，将信息简单地传递到父节点或指向目的节点的子孙节点。

网状拓扑结构与树形拓扑结构相同，但它的网络通信更加灵活。所有路由器都可以直接相互通信，而不需要先将信息发送到父设备。例如，如果设备 J 欲将信息发送到设备 K，那么可能的路由包括 J→I→ L→K、J→I →M→K、J→I→M→N→K、J→I→L→N→K 和 J→I→L→M→N→K。当某些路由失效时，网络路由算法会从可用的路由中选择替代路由。

2. 4. 2. 2　ZigBee 混合网络

通过适当使用星形、树形和网状拓扑结构，或它们的组合，ZigBee 网络可以形成不同的网络结构。其中的网状拓扑结构是最流行的网络拓扑结构，具有灵活的网络配置和自我修复网络通信的能力。

- 灵活的网络配置

从逻辑关系角度看，网状与树形有相同的拓扑结构。因为网状拓扑结构采用与树形拓扑结构相同的准则来构成网络，可以看做是一种特殊的树形拓扑结构。同时网状拓扑结构也是一种放大了的星形拓扑结构。由于路由器节点间可以相互启动通信，如果应用需要，可以通过编程方式使各通信流汇集到一个节点。因此，网状拓扑结构的网络配置非常灵活。然而，星形或树形网络不能扩展到网状网络。

- 自我修复能力

正如前文所讨论的，星形网络和树形网络有着共同的严重缺陷：如果路由或中心节点上的任何链接失败，整个网络就会崩溃。而网状网络使用动态路由协议绕过有故障的链路或节点来解决网络崩溃问题。

- 混合式结构

在通常的情况下，ZigBee 网络是混合式网络结构，而不是之前所讨论的 3 种结构中的任何一种。如图 2. 19 所示，ZigBee 网络由两层组成。第 1 层由 ZigBee 协调器和 ZigBee 路由器设备构成。路由器设备构成了网络的主干，在其内部实现了路

由协议。第 2 层由 ZigBee 终端设备构成，可以通过其父层的 ZigBee 路由器设备连接网络。根据 ZigBee 规范，一个 ZigBee 终端设备只能跟其父节点设备通信，因此，ZigBee 终端设备不涉及网络通信的转发功能。一个 ZigBee 终端设备和其他 ZigBee 网络设备之间的任何网络通信必须发送到相应的父设备，然后再路由到目的设备。父层 ZigBee 路由器设备与它所连接的 ZigBee 终端设备构成了星形网络拓扑结构。

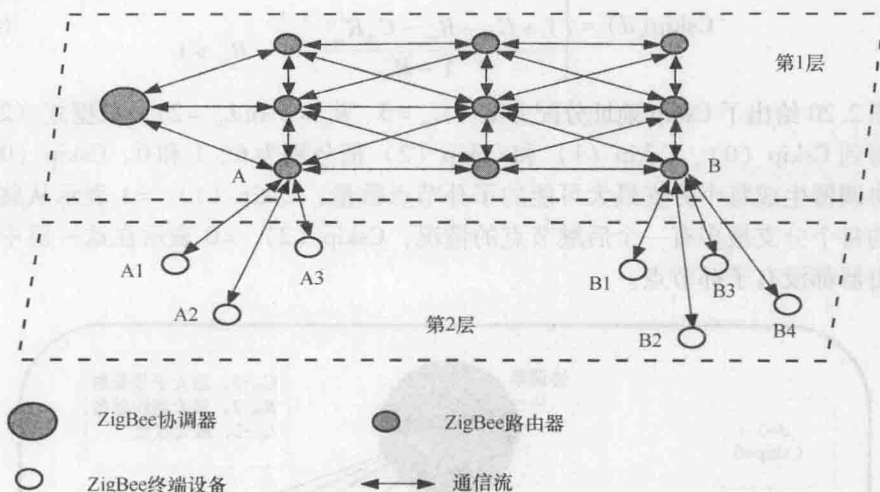


图 2.19　ZigBee 混合网络结构

2.4.3　ZigBee 地址分配方案

为了网络的应用，ZigBee 规范还定义了实际网络地址的分布式分配方案，并命名为“Cskip”。IEEE 802.15.4 标准对该方案没有说明。简单地说，一个树形拓扑结构的网络容量，即可用的 16 位地址的数量，由以下 4 个参数决定：

- C_m，每个父设备可以拥有子设备的总数。
- R_m，每个父设备可以拥有路由器总数。
- L_m，网络的最大深度（即父设备在哪一级可能不再有子设备）。
- d，设备的实际网络深度。

上述 4 个参数都存储在 ZigBee 协调器的网络信息库内。ZigBee 协调器根据 C_m 的大小为每个路由器分配一个地址块。路由器设备能接受的可允许的终端设备的数量可以按照下式进行计算：

$$\text{MaxEndDevices} = \text{MaxChildren} - \text{MaxRouters} = C_m - R_m \tag{2.5}$$

式中，当一个路由器设备成功加入网络时，它的父设备为其分配了地址块供它使用，该路由器设备也成了一个潜在的父设备。每个加入的路由器设备可以拥有一定

数量的子设备，其数量不能超过 C_m。新加入的路由器设备延长了网络的深度，但其深度不能大于 L_m。

如果终端设备成功加入网络，父设备会为它分配一个网络地址，但它不具有接受新的子设备功能。

Cskip 给出计算现有网络中任何分支可能的后继节点总数的方法，方法如下：

$$\mathrm{Cskip}(d)=\begin{cases}1+C_m(L_m-d-1) & R_m=1\\ \dfrac{1+C_m-R_m-C_mR_m^{L_m-d-1}}{1-R_m} & R_m>1\end{cases} \tag{2.6}$$

图 2.20 给出了 Cskip 地址分配方案（$C_m=5$、$R_m=2$ 和 $L_m=2$）。根据式（2.6），可以得到 Cskip（0）、Cskip（1）和 Cskip（2）值分别为 6、1 和 0。Cskip（0）表示从协调器生成每个分支最大可能的子孙节点数量，Cskip（1）=1 表示从路由器生成的每个分支最多有一个后继节点的情况，Cskip（2）=0 表示在这一层中的任何路由器都没有子孙节点。

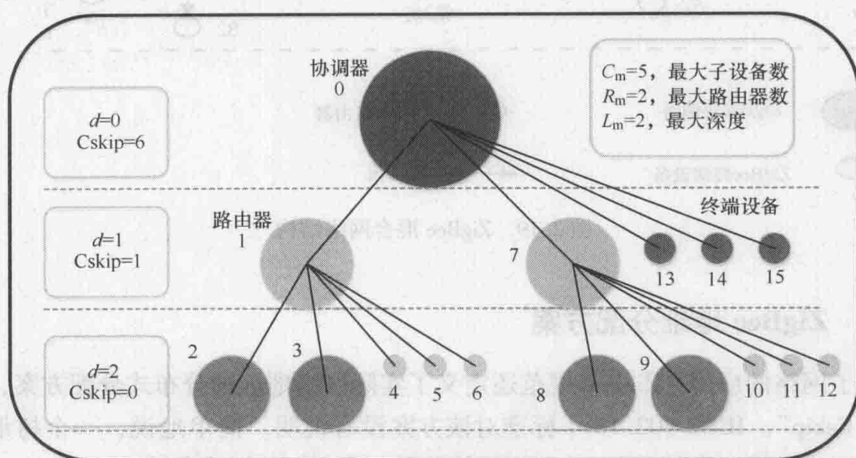


图 2.20 Cskip 地址分配方案（ZigBee，2008）

网络中可能的节点总数计算如下：

$$\mathrm{Node}_{total}=\mathrm{Cskip}(0)R_m+(C_m-R_m)+1 \tag{2.7}$$

表 2.6 给定不同参数时网络容量的计算（ZigBee，2008）

增 量 值	C_m	R_m	L_m	节 点 总 数
无	20	6	5	31101
C_m	21	6	5	32656
R_m	20	7	5	56021
L_m	20	6	6	186621

根据式（2.7），可以得到图 2.20 所示的节点总数为 $6\times2+(5-2)+1=16$，其中包括协调器的数量。一个网络中节点的最大数目随着 C_m、R_m 和 L_m 参数值的改变而变化。表 2.6 给出了给定不同参数（C_m、R_m 和 L_m）时网络容量的计算。当 ZigBee 设备加入 ZigBee 网络时，由 ZigBee 协调器或路由器为其分配一个 16 位逻辑地址。因此，在任何 ZigBee 网络中，网络节点的最大数目为 $2^{16}-1$（65535），表 2.6 中的最后一行是不切实际的。

Cskip（d）也通常作为地址偏移量分配给路由器和它的终端设备。假设已设定了协调器地址，那么第一个路由器 R_1 的地址等于协调器的地址 +1。通常使用下面的公式来给路由器 R_n 分配地址：

$$R_n=R_1+(n-1)\times\mathrm{Cskip}(d) \tag{2.8}$$

式中，d 为网络的深度，即协调器深度。每个路由器设备用同样的方式为每个子节点分配一个地址。例如，路由器 R_1 最初分配一个比自己地址大 1 的值给它的一个子设备。然后，路由器 R_1 使用 Cskip（$d+1$）作为地址偏移量分配给连接到 R_1 的其他子设备。其余的路由器也采用相同的分配过程。

ZigBee PRO 提供了随机分配地址方案。这意味着，每个节点加入网络时，就会在 0~65535 得到一个随机地址。如果该新地址已被现有的设备使用，就公告地址冲突并为其分配另一个新地址。

2.4.4　ZigBee 管理机制

ZigBee 标准的主要特点是为应用层提供了高效的管理机制。ZigBee 管理机制包括地址管理、描述管理、设备和服务的发现与绑定。

2.4.4.1　ZigBee 的地址管理

IEEE 802.15.4 标准用来构造 ZigBee 协议栈的底层（PHY 层和 MAC 层），ZigBee网络既可以使用 64 位扩展地址又可以使用 16 位网络地址。然而，这些还不能充分解决多个对象共享同一个物理地址的问题。在 ZigBee 规范中，可以用端点寻址的概念来解决此问题。

图 2.21 给出了 ZigBee 网络中的地址管理。图中有两个 ZigBee 设备 A 和 B，需要互相通信。设备 A 中的 3 个终端分别对应设备 B 中的 3 个传感器。如果设备 A 的终端 1 准备与设备 B 上的温度传感器建立通信，终端 1 通过使用 IEEE 802.15.4 标准的 64 位扩展地址或 16 位网络地址请求设备 A 与设备 B 建立无线通信信道。现在的问题是，设备 B 如何识别是与温度传感器进行通信的，而不是与另外两个传感器进行通信的。ZigBee 规范定义了一个子级寻址模式——端点，以帮助系统区分一台物理设备上的多个对象。“端点”是栈中虚拟存在的一种分类，每个 ZigBee 设备可以支持多达 240 个虚拟对象（端点 0 用于端点管理）。每个虚拟对象都有自己的属性，并独立于其他对象。如果通信的发起端指定了与其建立通信的端点，那么目标 ZigBee 设备中的 ZigBee 协议栈就可以轻松地确定目标对象。ZigBee 规范中

端点的概念非常有用，尤其对于 WSN。传感器节点通常配备有多个用于执行多个传感任务的传感器。

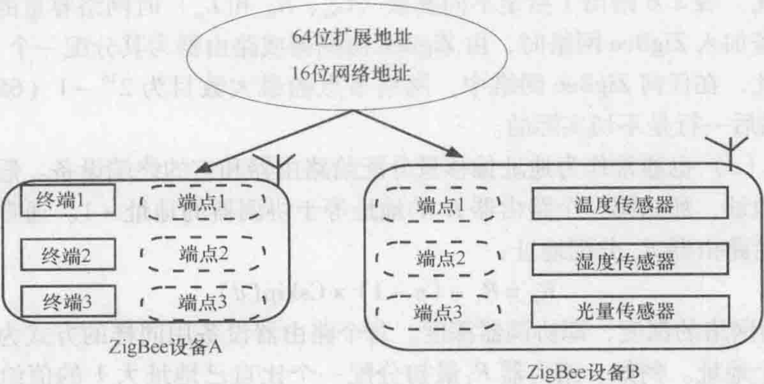


图 2.21　ZigBee 网络中的地址管理

2.4.4.2　ZigBee 描述管理

描述管理是 ZigBee 规范的通信基础，由信息、信息格式和处理动作方面的协议构成，其中已明确定义了能确保系统内合作的处理动作协议。通过遵循相同的描述，不同的组件能够创建互操作分布式应用。而且，不同厂商的产品可以无缝通信而不必担心兼容性问题。图 2.22 所示为 ZigBee 描述管理。

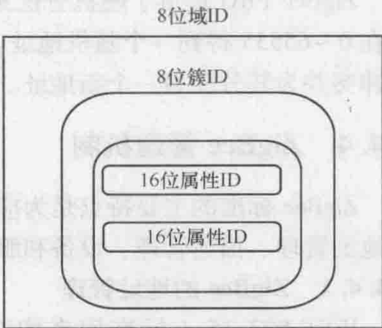


图 2.22　ZigBee 描述管理

在图 2.22 中，描述 ID 是一个长度为 8 位的数字，标识当前描述的属性。ZigBee 联盟已经指定了一些描述（智能家居协议栈、智能楼宇协议栈、工厂控制协议栈描述等），这些描述叫做公用描述。制造商可以为指定的应用定义属于它们自己描述，这些描述叫做私有描述。开发人员可以向 ZigBee 联盟申请描述 ID。为了管理方便，描述 ID 必须唯一。对于为了研究而定义的描述，用户不必申请使用许可。表 2.7 给出了 ZigBee 公有描述和相应的 ID。公有描述 ID 的范围为 0x0000 ~ 0x7FFF。私有描述 ID 的范围为 0xbf 00 ~ 0xFFFF。

表 2.7　ZigBee 公有域（Elahi 和 Gschwender，2009）

描　述　名	描述 ID
工业过程控制和监视（Industrial Process Control and Monitoring，IPM）	0x0101
智能家居（Home Automation，HA）	0x0104
商业楼宇管理（Commercial Building Management，CBM）	0x0105

（续）

描 述 名	描述 ID
电信应用（Telecom Applications，TA）	0x0107
个人、家庭和医疗（Personal、Home and Hospital Care，PHHC）	0x0108
先进的计量计划（Advance Metering Initiative，AMI）	0x0109

属性表示连接到节点的设备的功能或数据。例如，一个灯开关属性表示开关的位置（状态），可能是打开或关闭。属性标识符是用来指定 ZigBee 设备之间传送的实际数据项（即属性）的 16 位数字。

簇表示一组属性和用来执行特定功能的命令集合，其关联进出设备的数据流。例如，一个 SwitchOnOff 簇用来表示开或关的开关设备。簇标识符占 8 位长度，位于描述管理的第二层。在一个具体的描述中，簇标识符是唯一的。一个应用描述可以有多个簇。通过与描述 ID 相关联，属性 ID 可以表示应用的实际命令。

图 2.23 给出了使用 ZigBee 描述管理的实例。在图 2.23 中，具有描述 ID 为 0x01 的灯开关描述用来管理照明系统。图中定义了两个簇：SwitchOnOff 和 LightStatus。簇 SwitchOnOff 用于控制用户指令的执行情况。通过识别包含相应簇 ID 和属性 ID 的输入命令，本地系统能够正确执行打开或关闭指令。簇 LightStatus 用于表示接收到用户请求时灯的状态。通过检查包含簇 ID（LightStatus）和属性 ID（灯 ON/OFF）的格式消息，用户可以得到灯的当前状态。

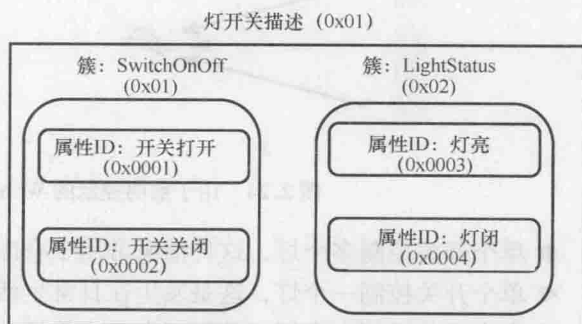


图 2.23　使用 ZigBee 描述管理的实例

2.4.4.3　设备和服务的发现

为了简化和标准化提供服务的方式，ZigBee 规范规定了发现网络中设备和服务的机制。设备发现命令同时支持 IEEE 64 位和 16 位网络地址，可以用于广播或单播。网络应有一个用于存储休眠模式下设备的节点描述符的主发现缓存设备，可以是路由器或者协调器。任何设备进入休眠模式前，发送其描述符信息给主发现缓存，主发现缓存设备响应进入休眠模式设备的请求，由 ZigBee 设备对象（ZigBee Device Object，ZDO）执行真正实现。例如，如果一个新加入网络的 ZigBee 设备想获取 ZigBee 协调器的网络地址，但是仅知道协调器的 64 位扩展 MAC 地址，或者一个设备想获取能提供控制灯功能的设备网络地址，那么 ZDO 可以向网络发送格式广播查询，或者向指定的设备发送一个单播查询，并且在查询结束后可以获得需要的结果。ZDO 是定义在 ZigBee 协议栈中的一种协议。运行 ZigBee 协议栈的每个

ZigBee 设备都有它自己的 ZDO 实例，可以在 ZDO 管理下完成信息处理，而不需要用户的干预。开发者要考虑的是如何设计查询提交和处理返回的结果。

2.4.4.4 ZigBee 绑定

ZigBee 规范中一个非常有用的功能是支持绑定的概念，即两个位于不同设备的端点间的逻辑关系。在传感器网络应用的开发过程中，发送控制消息经常会遇到以下情况：从单点到多目的或从多目的到单点，或从单点到单目的。用于照明控制的 WSN 信息发送如图 2.24 所示，有以下三种情况：

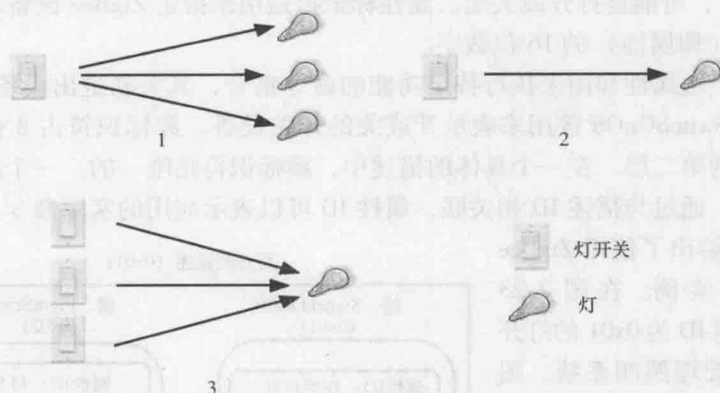


图 2.24 用于照明控制的 WSN 信息发送

- 单个开关控制多个灯，这种情况常用于仓库里中心开关的设计。
- 单个开关控制一个灯，这是发生在日常生活中的通常情况。
- 多个开关控制一个灯，常用于走廊或楼梯的控制灯的设计。

采用传统方法处理图 2.24 所示的过程需要大量的重复工作，而绑定机制可以使得完成上面的功能更简便。图 2.25 给出了 ZigBee 网络中绑定的实现过程。

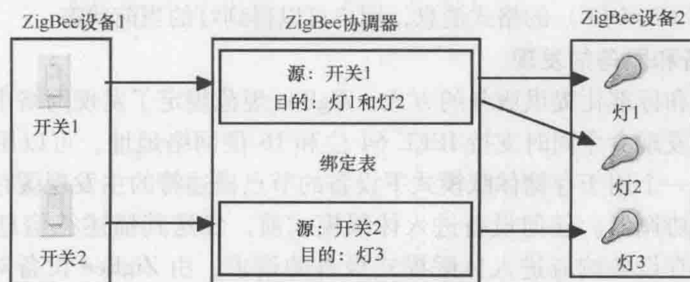


图 2.25 ZigBee 网络中绑定的实现过程

在图 2.25 中，在整个网络生命周期内，由于协调器始终处于工作状态，因此用于存储绑定表。在绑定表中需要建立并记录两项内容：第 1 项是记录开关 1 的端点和源地址，以及灯 1 和灯 2 的端点和匹配的地址；第 2 项记录开关 2 的端点和地

址，以及灯 3 的端点及匹配的地址。如果开关 1 需要开启灯 1 和灯 2，那么开关 1 就向协调器发送指令和它自己的地址。协调器一收到指令就搜索绑定表，并找出灯 1 和灯 2 的地址。然后，协调器用灯 1 和灯 2 的地址替换指令的目标地址，并自动地将指令发送出去。因此，开关 1 可以通过它们之间的绑定控制灯 1 和灯 2。并且指令可以被快速地处理，从而提高整体的执行效率。

2.5　6LoWPAN 和无线传感器网络

6LoWPAN 表示基于 IEEE 802.15.4 实现 IPv6 通信的低功率无线个人局域网（Low-power Personal Area Network，LWPAN），于 2007 年由因特网工程任务组（Internet Engineering Task Force，IETF）开发（Kushalnagar 等，2007）。IPv6 是因特网协议的最新版本。6LoWPAN 使 IPv6 能直接基于 IEEE 802.15.4 低功率 WSN 进行工作。因此，在基于 6LoWPAN 的 WSN 中，无线节点易于接入因特网。Shelby 和 Bormann（2009）为 6LoWPAN 给出了一个简明的技术定义，6LoWPAN 标准通过对相关协议的优化有助于基于低功率、低速率无线网络的 IPv6 在简单嵌入式设备的适配层上的有效使用。

WSN 应用于因特网的优势包括以下几项：

- 因允许使用基于 IP 协议的现有网络架构，可以实现互操作。
- 无线设备可以很容易地连接到因特网上而不需要网关。
- IP 的启用使得网络可以使用所有基于 IP 的技术，如代理服务。众所周知，代理服务可以用于大规模网络中的高级服务。
- 可以使用如 HTTP、SNMP 和 DPWS 等已建立的应用协议和数据模型。
- 通过使用传输协议对具有不可靠连接的网络提供一定的可靠性。
- IP 技术通过提供所有的标准和相关的可用文档促进了创新。
- 许多用于调试和设计的协议都是基于 IP 网络的。

图 2.26 给出了 6LoWPAN 协议栈结构，在 MAC 层和 IPv6 网络层之间增加了一个适配层或者叫做 LoWPAN 层。适配层的功能是执行下列任务：

- IPv6 头的压缩。
- IPv6 载荷的分片。
- UDP 头的压缩。

详细内容见 6LoWPAN 的规范定义（Kushalnagar 等，2007）。6LoWPAN 中也使用了用户数据包协议（UDP）和因特网信报控制协议（Internet Control Message Protocol，ICMP）。6LoWPAN 边界上的路由器在 IPv6 和 IEEE 802.15.4 之间的适配层上运行，该路由器称为边界路由器。

应用协议	
UDP	ICMP
IPv6	
LoWPAN	
IEEE 802.15.4 MAC	
IEEE 802.15.4 PHY	

图 2.26　6LoWPAN 协议栈结构

图 2.27 所示为 6LoWPAN 配置实例，给出了

WSN和因特网互联时边界路由器的位置。每个LoWPAN由一个边界路由器，若干LoWPAN路由器（R）和若干主机（H）组成。另外，在因特网上还有一个远程服务器。6LoWPAN通过有效压缩数据包头和简化IPv6需求使得IPv6适用于基于低功耗无线网络的简单的嵌入式设备。当将LoWPAN连接至因特网或另一个IP网络中时，还需要进一步考虑下面的一些问题（Shelby和Bormann，2009）：

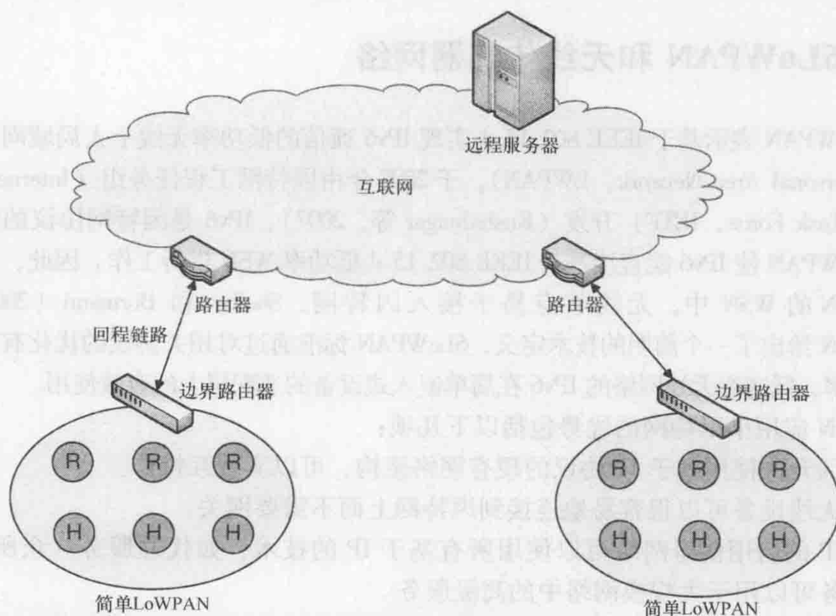


图2.27 6LoWPAN配置实例

● 最大传输单元，6LoWPAN的应用应该使数据包尽可能的小，避免把LoWPAN数据包分割为若干个IPv6数据包。

● 应用协议，端对端应用协议应该利用UDP和紧凑载荷格式以适应6LoWPAN节点的使用。

● 防火墙和网址转换，当6LoWPAN连接至因特网时，防火墙和网址转换问题是不可避免的。

● IPv4互联，目前IPv4和IPv6都在因特网上使用，6LoWPAN和IPv4节点或IPv4网络交互是必然的。

● 安全，将6LoWPAN节点连接至因特网中使得优点和风险共存。安全应该作为一个主要问题得到重视。

2.6 小结

本章介绍了WSN的基本标准和协议，尤其是IEEE 802.15.4、ZigBee和

6LoWPAN。ZigBee 和 6LoWPAN 都位于 IEEE 802.15.4 之上，所以 IEEE 802.15.4 为低速率、低功率的 WSN 奠定了基础。

WSN 的开发者常要处理 ZigBee 和 6LoWPAN 栈，而不是 IEEE 802.15.4 栈。这两种 LoWPAN 栈是最常用的，目前是彼此独立的。由于缺乏本地 IP 栈的处理能力，ZigBee 不能直接和因特网通信。目前有几种 6LoWPAN 和 ZigBee 互联的研究方法。第一种方法是将 IPv6 栈置于 ZigBee 网络层之上，将全局单播 IPv6 地址分配给每一个 ZigBee 节点；反之，是将 ZigBee 短地址分配给每个 IPv6 节点。网关负责处理所有网络流量的发送和接收，然后再处理所有分别进出 IPv6 网络或 WAN 的数据包的封装和解封（Wang 等，2007）。第二种方法是双栈系统的设计，6LoWPAN 和 ZigBee 栈均工作在同一 IEEE 802.15.4 MAC 层上。这种方法允许 6LoWPAN 和 ZigBee 栈共存于同一 IEEE 802.15.4 MAC 层上。尽管这种方法可以使 IPv6 和 ZigBee 的功能都应用在同一个节点上，然而任何时刻只能使用一个协议。最后，需要一个能将 6LoWPAN 和 ZigBee 设备转换成 IPv6 的网关（Hossen 等，2010）。

参考文献

Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cyirci, E.: A survey on sensor networks. IEEE Commun. Mag. **40**(8), 102–114 (2002)

Aschenbernner, J.R.: Open systems interconnection. IBM Syst. J. **25**(3/4), 369–379 (1986)

Elahi, A., Gschwender, A.: ZigBee Wireless Sensor and Control Network. Prentice Hall, NJ (2009)

Gutierrez, J.A., Callaway, E.H., Barrett, R.L.: Low-Rate Wireless Personal Area Networks Enabling Wireless Sensors with IEEE 802.15.4. IEEE Press, New York (2004)

Hossen, M.S., Kabir, A.F.M.S., Khan, R.H., Azfar, A.: Interconnection between 802.15.4 devices and IPv6: impleications and existing approachs. Int. J. Comput. Sci. **7**(1), 19–31 (2010)

IEEE: Part 15.4: Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LR-WPANs) (2003)

Kushalnagar, N., Montenegro, G., Schumacher, C.: IPv6 over low-power wireless personal area networks (6LoWPANs): Overview, assumptions, problem statement, and goals. RFC4919, Internet Engineering Task Force (2007)

Lewis, F.L.: Smart environments: Technology, protocol and applications. In: Cook, D.J., Das, S.K. (eds.) Wireless Sensor Networks, 1st edn, pp. 13–46. Wiley, New York (2004)

Nicopolitidis, P., Obaidat, M.S., Papadimitriou, G.I., Pomportsis, A.S.: Wireless Networks. Wiley, New York (2003)

Schurgers, C., Srivastava, M.B.: Energy efficient routing wireless sensor networks. In: Military Communications Conference on Communications for Network-Centric Operations: Creating the Information Force, vol. 1, pp. 357–361

Shelby, Z., Bormann, C.: 6LoWPAN—The Wireless Embedded Internet. Wiley, New York (2009)

Wang, R.C., Chang, R.S., Chao, H.C.: Internetworking between ZigBee/802.15.4 and IPv6/802.3 Network. In: SigComm Conference on IPv6 (IPv6'07), Kyoto, Japan

ZigBee: ZigBee specification, version 1.0. Available at www.zigbee.org (2004)

ZigBee: ZigBee stack advanced user guide, JN-UG-3045 Revision 1.2, 6 Mar 2008

第3章　无线传感器网络的硬件设计

关键词：微处理器　传感器　硬件设计　电源管理　能量捕获

3.1　通用无线传感器网络节点体系结构

建立任何 WSN 的首要任务是建立传感器节点，传感器节点必须满足特定应用的众多要求。由于 WSN 中采用大量的传感器节点，所以传感器节点应该是小的廉价的节能的，并有足够的存储、计算和通信能力。由于尺寸的限制，传感器节点不可以使用持久、大容量的电池或主电源作为它们的电源。基于低成本和节能方面的要求，传感器节点应使用低功耗处理器，使用有限带宽和传输范围的小型无线收发器。因此，传感器节点的设计受到所需计算能力和通信能力的限制。通常情况下，传感器节点由以下 4 个主要的子系统构成：

- 传感子系统，包括一个或多个监视物理环境的传感器和执行器。
- 计算子系统，由微控制器或具有存储器的微处理器构成。其中，存储器用来存储和处理由传感子系统收集的数据。
- 通信子系统，由用于无线数据通信的短程无线系统构成。
- 电源子系统，通常使用电池为整个传感器节点供电。如果引进能量捕获技术，发电设备可能会应用于电源子系统。

典型的无线传感器节点结构如图 3.1 所示。传感子系统可以分为两部分。第一部分是一个基本传感装置，包括传感器，能从节点周围的物理环境中获取信息，并将其转换成模拟信号，然后经模-数转换器（Analogue-Digital Converter，A-DC）将这个模拟信号转换成数字信号。第二部分是一个智能传感装置，可以提供附加的功能，如对采样数据进行预处理，或者对测量误差进行补偿。传感子系统必须提供一

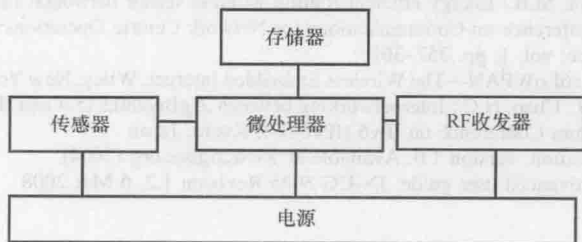


图 3.1　典型的无线传感器节点结构

个接口以便与由微处理器执行的计算任务兼容。

计算子系统执行所有的计算工作，如处理传感数据、实现数据融合、管理系统电池的操作、设置传感器的参数，并执行高层协议，如 ZigBee 规范。在本子系统中能耗主要来自于微处理器。工作在一个较低的电压是一种降低功耗的解决方案。另外一种方案是将子系统的工作周期划分成不同的模式，系统在这些模式间进行切换，以保证微处理器总是在省电模式下运行。

通信子系统负责发送和接收数据帧。众所周知，发射器消耗的大部分能量用于无线通信，并且通信距离取决于发射功率。大多数射频（Radio Frequency，RF）模块提供了一种由程序按照要求控制发射功率的机制，以使能量更有效地使用。

电源子系统由电池和含有辅助控制电路的直流到直流（DC-DC）的转换器构成。DC-DC 转换器提供多种不同电压来支持系统中的所有设备，这样可以使它们在不同的模式下工作，从而可以减少功耗。

3.2 片上系统和基于组件设计

利用市场上提供的 RF 模块来设计无线传感节点有两种方法：一种是基于片上系统（System on Chip，SoC）的解决方案；另一种是基于组件设计的解决方案。许多 RF 模块制造商，如挪威 Chipcon 公司、美国 Microchip 公司和 Freescale 公司及其他很多制造商，都提供带 SoC 的 RF 模块。该模块在一个芯片上集成了微处理器、闪存、RAM、A-DC 及一些特殊的电子电路。这些 SoC RF 模块使无线传感器节点的硬件设计变得快速、简单、可靠，因为在设计中只需要添加一些额外的组件。SoC 解决方案的缺点是缺乏灵活性，一些特殊的要求可能难以满足。基于组件设计的方法为设计人员提供了全面的灵活性，设计人员可以选择所需要的所有组件，如 RF 模块、微处理器和其他电子元器件，并根据所选择的部件来为传感器节点设计不同的布局。因此这种方案可以实现更低的成本和更高的性能，但是也可能更复杂和费时。本章重点介绍了采用兼容 ZigBee 的 SoC 设计方案，因为它可以显著缩短市场化的时间。为了方便参考，表 3.1 给出了常用 ZigBee 芯片的对比。

表 3.1 常用 ZigBee 芯片的对比

制 造 商	产品编号	电源电压 /V	休眠电流 /μA	发射电流 /mA	接收电流 /mA	发射功率 /dBm	接收灵敏度 /dBm
美国 Atmel 公司	AT86RF231	1.3 ~ 3.6	0.02	14.3	13.2	3	-101
美国 Freescale 公司	MC13192	2.0 ~ 3.4	1	30	37	4	-91
美国 Texas Instruments 公司	CC2420	2.1 ~ 3.6	20	17.4	18.8	0	-95
挪威 Microchip 公司	MRF2J40	2.4 ~ 3.6	2	19	23	0	-95
英国 Jennic 公司	JN5139	2.7 ~ 3.6	2.6	37	37	2.5	-96

（续）

制　造　商	产品编号	电源电压 /V	休眠电流 /μA	发射电流 /mA	接收电流 /mA	发射功率 /dBm	接收灵敏度 /dBm
美国 Ember 公司	EM2420	2.1～3.6	0.5	17.4	19.7	10	-94
瑞士 ST 公司	SN260	2.1～3.6	1.0	35.5	35.5	2.5	-100

表3.1中，美国Jennic公司的JN5139芯片将在本章的研究设计案例中使用。作为一个典型的SoC解决方案，JN5139模块集成了所需的所有2.4 GHz RF组件。它由一个JN5139微处理器、1Mbit串行闪存和外围电路组成。1Mbit串行闪存用来存放启动过程中加载到微处理器的应用程序代码。Jennic模块不需要进行昂贵的RF设计和测试。传感器节点可以通过向Jennic模块供电，以及将开关、执行器和传感器与I/O引脚进行连接的方式进行简单地设计。JN5139模块的框图如图3.2所示。该模块由一个32位的精简指令集计算机（Reduced Instruction Set Computer，RISC）CPU、存储器系统、丰富的模拟和数字外围设备，以及一个兼容IEEE 802.15.4标准的2.4 GHz收发器组成，并集成在同一块芯片上。

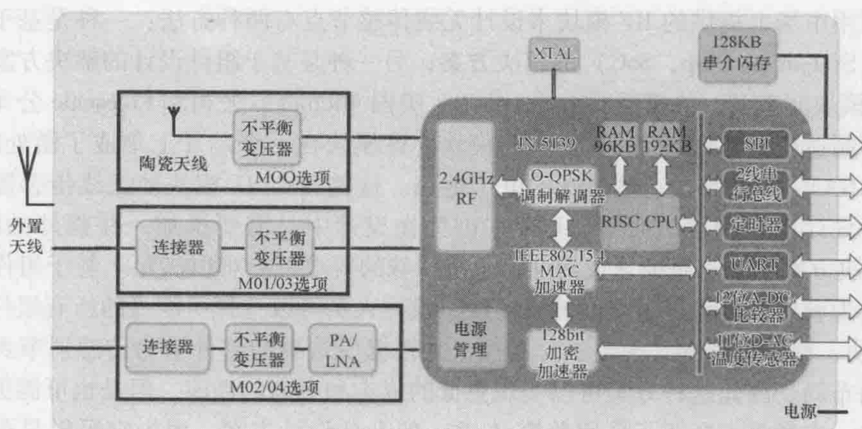


图3.2　JN5139模块框图

3.3　设计准则

在WSN硬件设计中，必须考虑到以下设计准则：

● 寿命。在许多应用中，传感器节点被部署在人们可能很难进入的地方。而且传感器节点的寿命又依赖最初提供给它的有限的电源，因此定期更换WSN电池是不可行的。在WSN硬件设计中，为了使整个网络的寿命最大化，每个节点的设计都必须能够控制自己的功耗。因此，每个电路的设计应保证最小的功率消耗。另

外，在传感器节点上提供能量捕获单元也可以增加 WSN 的寿命。

● 覆盖范围。WSN 必须覆盖的目标区域，即覆盖范围，由具体的应用需求决定。发射功率和传感器节点的部署应由覆盖范围的需求确定。当覆盖范围变大时，传感器节点将消耗更多的功率用于数据采集和传输，这意味着该 WSN 的寿命将因为有限的功率供给而被缩短。

● 鲁棒性。无线传感器节点可能需要在不确定的或恶劣的环境中工作。WSN 的设计必须可以承受和适应个别节点故障，从而当某个节点发生故障时，WSN 还能从整体上保持功能。

● 通信。传感器节点应具有低通信数据率和低通信功耗。

● 时间同步。为了节能，传感器节点应该在完成任务后就保持在休眠模式下，并且必须能够周期性地或按需被唤醒。精确的时间同步可以使传感器节点与网络中的其他节点之间协同工作。

● 安全性。WSN 的一些应用（如许多军事应用）要求数据保密，因此 WSN 必须能够实现安全算法。因此，选择用于各个传感器节点的微处理器必须能够执行复杂的加密和认证算法。

● 成本和尺寸。WSN 的部署可能需要上千个传感器节点。单个传感器节点的成本和尺寸应该做到最小，从而保证此部署的经济性。

基于上述考虑，无线传感器节点的硬件设计可以分为以下步骤：微处理器的选择、RF 通信设备的选择、传感单元的设计，以及电源单元的设计。

3.3.1　微处理器的选择

微处理器是传感器节点的核心部件，负责收集、处理、压缩、记录和存储数据。一般来说，一个 SoC 微处理器在一块芯片上集成了 CPU、闪存、RAM、模拟和数字外设。使用 SoC 微处理器进行传感器节点的设计可以减少设计和测试的成本，是 WSN 的理想选择。在选择正确类型的微处理器时，还需要考虑如下实际性能参数：

● 性能。微处理器的性能水平可以显著影响传感器节点的功耗。这是因为具有更好性能的微处理器需要更多的功耗。由于对微处理器性能的要求因应用的不同而不同，所以 WSN 系统中理想的微处理器性能应该以满足应用的性能需求为标准，而不是选择性能最佳的微处理器。

● 操作模式。为了节能，微处理器通常有不同的操作模式，包括活动、空闲和休眠模式，其中每个模式具有不同的功耗。进入和退出休眠模式的转换次数是决定传感器节点总功耗的重要因素。微处理器进入和离开休眠模式越快，它处于休眠模式的时间就越长，整个节点能耗就越少。因此，不同的模式的功耗水平、转换次数、转换功率和微处理器在每个模式下花费的时间，都对传感器节点的总能耗有显著的影响。

● 电压要求。微处理器的工作电压范围可以对系统的性能和传感器的选择产生显著影响。通常选择工作范围为 2.7~3.3V 的传统低电压微处理器。

● CPU 速度。因为微处理器的功耗与频率呈线性关系，CPU 的最佳速率是由数据分析和节点必须完成的网内处理的工作量所决定的。

● 外围设备支持。由于微处理器的设计专门用来与外部设备进行交互，它应该具有通用的数字 I/O 引脚、A-DC、比较器和数字接口（如 RS-232、UART、I2C 或者 SPI 等）。

● 存储器。根据 WSN 应用程序的大小，微处理器应具有足够大的存储空间来承载应用程序。程序通常驻留在闪存中，微处理器在启动阶段，可以对其进行擦写。

● 软件支持。可用的软件库也可以影响微处理器的选择。例如，许多研究人员和工程师更喜欢用 C 或 C++编写自己的代码。因此，能支持这些软件开发环境的微处理器被认为是一种理想的选择。

● 成本和尺寸。低成本和紧凑的尺寸是选择微处理器时另一个要考虑的因素。通常的情况是选择集成了 MCU 和 RF 模块的芯片，因为其成本低、体积小而且易于开发。

3.3.2　通信设备选择

通信设备用于传感器节点之间的交换数据。通常，通信设备由一个低功率无线电系统组成，该系统包括一个 RF 收发器（天线）、功率放大器和数字基带。无线电系统通常是 WSN 中功耗最大的部件，因此优化其功耗可显著改善整个系统的寿命。影响无线电系统的选择主要有以下几个方面。

● 无线技术。有一些无线技术可供商业应用，如 ZigBee、Wi-Fi 和蓝牙（见表 3.2）通常 WSN 选择基于 ZigBee 技术来实现短距离、低功率、低数据吞吐量、低成本、体积小的简单无线通信系统。

表 3.2　ZigBee、Wi-Fi 和蓝牙的无线技术比较

名　标	ZigBee	Wi-Fi	蓝　牙
标准	802.15.4	802.11a，b，g	802.15.1
系统资源	50～60KB	>1MB	>250KB
电池寿命/天	100～1000	1～5	1～7
网络规范	65536	32	7
带宽/(kb/s)	20～250	11000	720
最大传输范围/m	100 以上	100	10
安全性	128 AES 和应用层安全	—	64 位和 128 位加密
工作频率	868MHz（欧洲） 900～928MHz（北美） 2.4GHz（世界）	2.4GHz 和 5GHz	2.4GHz

● 传输范围。无线传输范围决定了任意两个传感器节点之间的最短距离，从而也决定 WSN 的覆盖范围。还有一些影响无线传输范围的因素，如传输功率、收

发器的传输范围、接收器灵敏度、天线的增益和效率及信道编码机制。优化传输功率可以大幅节省传感器节点的能耗。较高的传输功率可以获得较高的信噪比（Signal-to-Noise Ratio，SNR）和较低的误码率（Bit Error Rate，BER）。而且，信号传输的能量越大，信号传输得就越远。这样不仅可以增加覆盖范围，而且可以减少来自其他无线系统的干扰。设置大小合适的传输功率是至关重要的，因为这样既能确保获得满意的通信质量和覆盖范围，又能达到合理的能耗。通常情况下，Ad-hoc WSN 首选全向天线，因为它们允许节点在各个方向上进行有效的通信。

● 调制类型。RF 通信设备的一个功能是将数字信号转换成用于传输的模拟信号，这个过程被称为调制。标准的调制机制包括，幅度调制［如幅移键控（Amplitude Shift keying，ASK）］、频率调制［如频移键控（Frequency Shift Keying，FSK）］和相位调制［如相移键控（Phase Shift Keying，PSK）］。ASK 采用振幅的变化来代表 0 和 1。FSK 使用频率的变化来表示 0 和 1。PSK 使用信号的相位来表示二进制数据。通常，WSN 选择正交相移键控（Quadrature Phase Shift Keying，QPSK）调制技术，它是将每个信号按照 90 度增量进行移相。

● 比特率。和其他许多高性能数据网络不同，WSN 不需要高比特率通信。10 ~ 200kbit/s 的原始网络带宽通常能满足大多数应用。

● 启动时间。无线电系统快速进入和退出低功耗的休眠模式的能力，对 WSN 的高效运行非常重要。如果一个无线电的导通到接收时间超过几十毫秒，它将不可能达到所需的小于 1% 的占空比。其中，占空比定义为系统处于工作状态的时间与总时间的比值。

3.3.3 传感器设计

传感器是一种测量物理量并且将其转换为电信号的设备，转换后的电信号可由其他电子设备来读取。它在物理环境和电子设备之间提供了接口。传感器有许多分类方法。从电源的角度来看，传感器可以被分为两大类：无源传感器和有源传感器。无源传感器不需要任何额外的电源，由外部激励直接产生电信号，如光敏二极管。有源传感器需要外部电源才能进行工作，如热敏电阻器。就传感器输出的信号类型而言，传感器可分为数字传感器和模拟传感器。数字传感器将二进制值输出到微处理器；模拟传感器将外部变量转换为模拟信号，通常是一个电压值。传感器的第三种分类方法是基于测量的内容的，可分为热传感器、机械传感器、化学传感器、磁性传感器、辐射传感器和电传感器。表 3.3 给出了 WSN 中使用的传感器类型和转换原理。这些传感器可以部署在被测对象的内部或附近。

一个理想的传感器应具有高灵敏度、高准确度和可重复性，以及低功耗和成本，同时易于使用。但是，传感器通常很难兼顾以上所有的优势，所以在 WSN 的设计中必须选择特定应用的传感器。在传感器的选择过程中应该考虑以下三个方面因素：

● 环境条件，如工作温度、压力、光、湿度和放置传感器节点的位置。

● 设计参数，如测量的目的、输出信号的类型、使用的数据传输技术、使用的微处理器、所需的信号调节技术。

● 传感器参数，包括传感器封装的尺寸、被测环境变化的响应时间、测量的准确性、转换器寿命、功率需求、可用的配件、测量范围、最大误差容限、转换器的激励电压、激励电源的电流及成本。

表 3.3 WSN 中使用的传感器类型和转换原理（Cook 和 Das，2004）

测 量 量	转 换 原 理
物理式	
压力	压阻式，电容式
温度	热敏电阻，热-机械，热电偶
湿度	阻性，容性
流量	压力变化，热敏电阻
位移式	
位置	磁场，图像，GPS，接触式传感器
速度	多普勒，霍尔效应，光电效应
角速度	光编码器
加速度	压阻式，压电式，光纤
接触式	
应变	压阻式
力	压电式，压阻式
扭矩	压阻式，光电效应
滑动	双力矩
振动	压阻式，压电式，光纤，声，超声
存在式	
触觉/接触	触点开关，电容式
接近	霍尔效应，电容式，磁，地震学，声学，射频
距离/范围	磁场（声呐，雷达，激光雷达），磁，隧道
移动	磁场，红外，声学，地震（振动）
生化式	
生化试剂	生化传导
识别式	
个人特征	视力
个人 ID	指纹，视网膜扫描，声音，热羽流，视觉分析

下面列出了对典型传感器的一系列需求。任何一个应用需求可以由其中的一个或多个构成。表 3.4 给出了常用的传感器技术规范（Ristic，1994）。

表 3.4　常用的传感器技术规范

参　数	说　明
绝对灵敏度	输出变量对输入变量的比值（物理或化学量）
相对灵敏度	输出变量与被测变量经被测变量为 0 时输出量归一化后的比值
交叉灵敏度	由多个被测量导致的输出量变化
方向依赖灵敏度	对被测量和传感器之间角度依赖的灵敏度
精度	传感器能检测到的最小输入增量
准确度	输出信号最大误差与满量程输出信号以百分比表示的比值
线性误差	输出信号的校正曲线与描述输出信号的最佳拟合曲线之间最大的偏差
迟滞	对于给定的测量值，传感器在正、反行程中输出的信号不相同
偏移	当被测量为 0 时的输出量
噪声	与被测量无关的随机信号
截止频率	输出信号降低到最大值的 70.7% 时的频率
动态范围	传感器可以测量的最大值和最小值之间的范围
工作温度范围	传感器输出信号能够保持在规定的误差内的工作温度范围

- 传感器应该考虑成本效益，并且安装造价合理。
- 传感器的操作和维护应该很容易进行，不需要进行特殊培训。
- 传感器应该能够在要求的时间范围内能够连续可靠地工作，并且重新部署或更新时价格合理。
- 微处理器能够控制传感器。
- 传感器应是小尺寸和轻便的以便携带。
- 传感器如果是电池驱动，应节能，即具有较少的能耗。
- 传感器应能在危险场所和/或恶劣环境下使用。

3.3.4　电源设计

电源是无线传感器节点的重要组成部分。WSN 的大多数传感器节点是电池驱动的，所选择的电池的寿命直接决定了传感器节点的寿命。电池的寿命是由电池的尺寸、所用的电极材料的类型及在电解液中的活性物质的扩散速度决定的。在为传感器节点选择电源时，应该考虑平均电流消耗、最大电流消耗及电池的成本。

平均电流消耗：传感器节点的平均电流消耗是影响电池选择的最主要的因素。电池释放的电流随传感器节点的状态而变化。为了计算平均电流，有必要确定传感器节点每个状态的耗电量及每个状态所花费的时间。每个传感器节点的平均消耗电流 I_{average} 可以用下面的公式来确定：

$$I_{\text{average}} = I_1 \frac{t_{\text{on1}}}{t_{\text{total}}} + I_2 \frac{t_{\text{on2}}}{t_{\text{total}}} + \cdots + I_n \frac{t_{\text{on}n}}{t_{\text{total}}} \tag{3.1}$$

式中，I_i，$i=1$，2，…，nI_i，为状态i消耗的电流；t_{oni}，$i=1$，2，…，n，为状态i消耗电流所需的时间；t_{total}为状态周期的总时长。

一旦计算出平均电流，就可以用下式来计算在期望的电池寿命内设备需要的电量：

$$I_{average}T_{runtime} \tag{3.2}$$

式中，$T_{runtime}$电池所需工作的时间，单位为h。此公式可以计算出传感器节点所需的最小能量。

最大电流消耗：每个电池都有一个制造商指定的额定电流量。电流太大超过额定值将显著减少电池寿命。因此，为了避免电池寿命下降，电池释放的电流应低于额定电流，并将额定电流作为最大电流消耗。

尺寸和成本：电池的尺寸和成本也是重要的因素，也应该给予被考虑。若要寻求一个低成本和小尺寸的电池设备，那么通常要检查备选电池的说明书。因为对于给定类型的电池性能，不同的制造商可能有很大的不同。

3.4 设计案例

本节将阐述一个用于安全监测的无线温度和一氧化碳（CO）传感器的设计案例。选择Jennic的JN5139作为微处理器和通信设备，以及两节AAA电池作为电源。下面重点讨论温度和CO传感器的选择，以及电路的设计。

3.4.1 温度传感器设计

市场上有许多不同类型的温度传感器，可以简单地分为四类：热电偶、电阻温度检测器（Resistance Temperature Detecor，RTD）、热敏电阻和集成电路（Integrated Circuit，IC）温度传感器。表3.5给出了4种温度传感器的比较。

表3.5 4种温度传感器的比较

属 性	热 电 偶	RTD	热 敏 电 阻	IC温度传感器
温度范围	-190～1821℃	-200～850℃	-90～130℃	-55～150℃
准确度	低	高	中等	高
反应时间	快	中等	快	快
稳定性	不稳定	长期稳定	中等	长期稳定
线性	中等	良	差	优
灵敏度	低	中等	较高	较高
互换性	中等	优	差	中等
重复性	差	良	中等	优
尺寸	小到大	中等到小	小到中等	小到中等

热电偶设备是由 Thomas Seebeck 于1822年发明的，通常用于制造工业温度计。它由两种不同的金属接合在一起，在给定的温度下产生一个很小的单一的电压值。通常，热电偶被认为是最小、最快和最持久的温度测量方案（Swanson，2010）。它可以被用于极宽的温度范围和恶劣的环境条件下。但是热电偶有3个缺点：首先，用热电偶测量温度需要测量2个温度；其次，被测温度和热电偶的输出电压之间的关系是非线性的；第三，由于测量的准确度不高，还需要一个特殊的补偿技术。

RTD 是一种正温度系数传感器，它包含一个电阻器，阻值随着温度的变化而变化。它具有高准确度、低漂移、工作范围广、重现性强和线性适中的优点。RTD 的局限性在于它不能被用于高温的应用，同时对小的温度变化不灵敏。当对测量的稳定性和准确度有严格要求时，RTD 是首选。

热敏电阻传感器也是阻值随温度变化的一类电阻器。但热敏电阻与 RTD 的区别是，热敏电阻使用的材料通常是陶瓷或聚合物，而 RTD 使用的是纯金属。最常见的热敏电阻具有负温度系数。它的特点包括温度范围适中、成本低、线性较差但可预知。热敏电阻是测量温度范围相对较窄和灵敏度高这类应用的首选传感器。

IC 传感器做成芯片的形式，是完全的硅基传感电路，拥有模拟或数字的输出。IC 温度传感器使用在 -55 ~ 150℃的温度范围内。与其他类型的温度传感器相比，它有许多优点。首先，IC 温度传感器是一种体积小、准确度高、价格便宜、具有极好线性度的温度传感器。其次，它们很容易与其他设备（如放大器和微处理器）相连接。

由于 IC 传感器具备一系列的优点，在本设计中选用美国 Maxim 公司的 IC 温度传感器 DS18B20。该 DS18B20 数字温度传感器提供 9 ~ 12 位摄氏温度的测量量，并具有非易失性、用户可编程及温度上下限触发点的报警功能。DS18B20 通过一条数据总线与中央处理器通信，特点如下：

- 电源范围，3.0 ~ 5.5V；
- 温度测量范围，-55 ~ +125℃；
- 精确性，-10 ~ 85℃范围内测量精度为 ±5℃；
- 传感器分辨率，9 ~ 12 位，可供用户选择；
- 可以在 750ms 内将温度转换成 12 位的数字值；
- 有 8 引脚 SO、8 引脚 SOP 和 3 引脚 TO-92 封装形式的芯片。

本设计中选用 3 引脚 TO-92 封装的芯片，DS18B20 引脚说明见表 3.6。该应用电路原理图如图 3.3 所示。DS18B20 的芯片由一个外部电源向 VDD 引脚供电。DQ 引脚被连接到微处理器的 DIO 引脚。

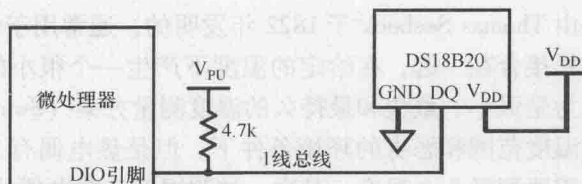


图 3.3　DS18B20 应用电路原理图（Dallas Semiconductor，2008）

表 3.6　DS18B20 引脚说明

DS18B20（TO-92）	名　称	功　能
1	GND	地
2	DQ	数据输入/输出
3	V_{DD}	可选的 V_{DD} 必须在寄生供电模式下接地工作

3.4.2　一氧化碳传感器设计

气体传感器广泛应用于空气中的有毒和可燃气体检测。它们与各种气体相互作用，从而触发电信号的输出。在气体传感器的选择中应考虑下面的过程：

● 确定目标气体及监测区域任何可能的背景气体。背景气体的存在可能导致气体传感器故障。

● 确定目标气体的浓度。一般的，测量气体的浓度和范围应为实际监测浓度的 3 ~ 5 倍。

● 确定安装气体传感器工作环境的温度范围。

● 确定可接受的功耗，因为很多气体传感器要求大电源。

● 确定气体传感所需的响应时间，因为很多气体传感器具有较长的响应时间。

● 确定可接受的成本和尺寸。

气体传感器可以分为电化学、半导体、催化剂和红外线。通常，电化学气体传感器有 2 个或 3 个电极与电解液接触。它们通过电极氧化或还原目标气体来测量其浓度。电化学反应会导致电流流过外部电路。该电流可以用外部放大电路来测量，此电流可以表示目标气体的浓度。电化学传感器的优点有封装紧凑、鲁棒性强、没有或几乎没有外部电源要求，以及大批量生产的成本低。但是电化学传感器的寿命往往不到 3 年，而且响应时间大约是 30s。更换传感器的成本很高，尤其是在大规模的部署中。电化学传感器主要用于检测有毒气体。

气体检测设备中的半导体气体传感器采用的是半导体。特定的气体可通过半导体的电特性变化来测定。半导体气体传感器的意义在于其诸多的优势，如尺寸小、寿命长、响应时间快和检测极低浓度气体的灵敏度高。但它们通常需要一根 5V 的外部电源，以确保传感器保持在工作状态。

催化式气体传感器包括一根如铂铱合金的引线嵌入在一个陶瓷珠中。催化式气体传感器使用加热的铂丝裸线圈燃烧目标气体，燃烧过程中所产生的热量使引线的电阻值发生变化。该电阻变化通过一个简单的惠斯顿电桥电路进行测量。这种传感器的设计非常简单，而且易于制造。使用这种技术的优点是它可以直接测量气体。但是，该传感器需要额外的功率来加热裸线圈，因此不适合用于电池驱动的传感器。催化式气体传感器主要用于检测可燃气体。

红外气体传感器被认为是一个“非反应”气体传感器。它的工作原理是基于该目标气体可以吸收通过它的光中的一部分红外线波长，而其他波长的光通过时不受影响。红外气体传感器使用红外光源照射一定量的气体，气体吸收的光量与目标气体的浓度有关。此技术的主要优点是寿命长、与目标气体无接触、高准确度和浓度测量可靠。然而红外气体传感器的缺点是高成本、高功耗。

在建立该安全监控的案例中，拟选择日本 Figaro 公司的 TGS5042 电化学 CO 传感器作为传感器节点，因为它本身不需要供电。TGS5042 CO 传感器的特点概述如下（Figaro，2010）：

- 电池供电；
- 对 CO 气体的重复性/选择性高；
- CO 气体的浓度与传感器信号输出呈线性关系；
- 易于校准；
- 寿命长；
- 目标气体为 CO；
- 典型检测范围为 0 ~ 10000 ppm㊀；
- CO 传感器的输出电流为 1.2 ~ 2.4nA/ppm；
- 工作温度范围为 -40 ~ +70℃；
- 响应时间为小于 60s。

图 3.4 给出了 TGS5042 应用电路原理图。传感器能产生一个极小的电流，经过放大器（OP-AMP）电阻电路转换为传感器的输出电压。该输出电压通过一个 A-DC 引脚送入 JN5139 模块。

3.4.3　传感器节点电路设计

图 3.3 所示的温度传感器和图 3.4 所示的 CO 气体传感器可以与微处理器集成在一电路中。图 3.5 所示为具有温度和 CO 气体传感器的传感器电路原理图。图左侧为作为微处理器和通信设备的 JN 5139 模块，CO 气体传感器和温度传感器电路位于右上角。右下角是承载两节 AAA 电池的电源电路。这个电路原理图可以转换

㊀ ppm：parts per million，百万分之一。此单位用于表示浓度比。

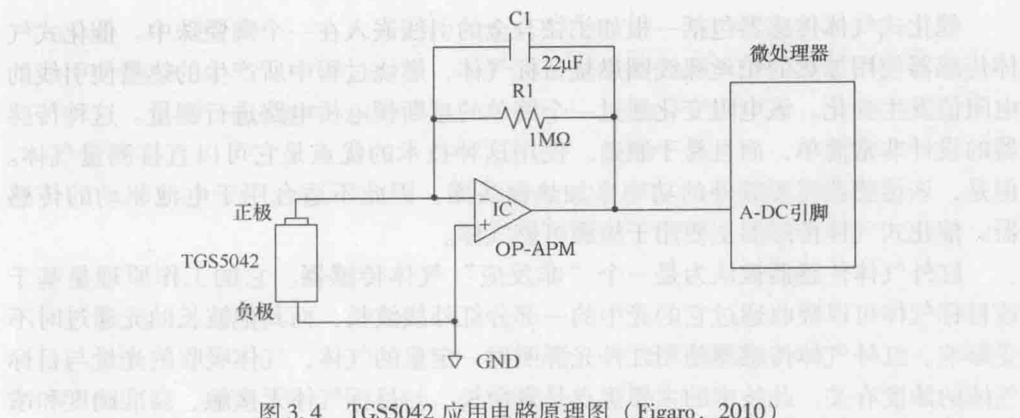


图 3.4 TGS5042 应用电路原理图（Figaro，2010）

为一个印制电路板（Printed Circuit Board，PCB）图，通过它可以制造具有温度和CO 气体传感器的无线传感器节点。组件和参数列表如表 3.7 所示。

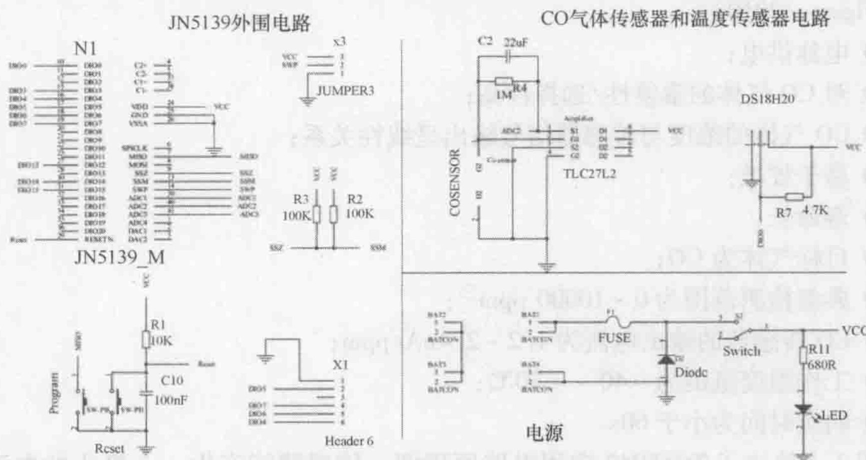


图 3.5 具有温度传感器和 CO 气体传感器的传感器节点电路原理图

表 3.7 组件和参数列表

指 示 符	说 明
J1	6 针管座 2.45mm
J2	3 针管座 2.45mm
BAT1-BAT4	电池座
R1	电阻 680kΩ
R2	电阻 100kΩ
R3	电阻 100kΩ
R4	电阻 10kΩ

（续）

指　示　符	说　明
R5	电阻4.7kΩ
R6	电阻1M
FUSE	500mA 熔丝
D1	BAS21 二极管
Ds1	LED
C1	电容100nF
C2	电容22μF
S2	开关
Program，Reset	按钮
U1	JN5139
U2	TGS5042 CO 传感器
U3	TLC27L2 运算放大器
U4	DS18B20 温度传感器

3.5　电源管理

电源管理是一种延长由电池驱动的传感器节点寿命的方式。它的目的是通过尽可能关闭电源或将传感器系统切换到低功率状态来避免能耗和提高能效。传感器节点的能耗可以分为“有用”和“浪费”两种。有用的能耗可以被用于环境感知、数据处理、数据的发送或接收、处理查询请求，以及向相邻节点转发查询和数据。在WSN中，能耗浪费可以发生在数据采集、数据处理和数据通信的过程中。因此，电源管理应处理这三个功能的能耗，如图3.6所示。但是，本节只涉及电源管理相关的硬件设计，即数据采集阶段的芯片级电源管理。数据处理和数据通信阶段的电源管理将在本书的后续章节中进行讨论。

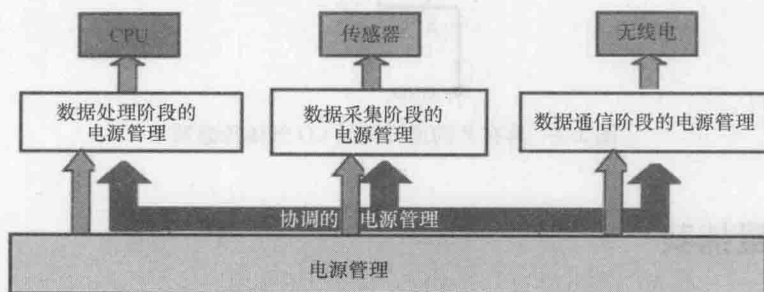


图3.6　传感器节点的电源管理

各个元器件的功耗是由电源的电压、各个元器件的电流消耗，以及它们的运行时间共同决定的。一旦选定了电子元器件，前两项便确定了。元器件的运行时间可以分为两部分——工作时间和空闲时间。元器件在空闲状态与工作状态消耗同样的能量。数据采集阶段的电源管理的任务是，节点在收到从微处理器发出的采集命令后打开传感器电源，在节点进入闲置状态时关闭电源。

对于图 3.5 所示温度传感器和 CO 气体传感器的电路，其中温度传感器 DS18B20 具有休眠模式，该模式的功耗为 0.003mW。在第 4 章将要介绍的传感器驱动器可以使温度传感器在没有传感任务时保持在休眠状态。CO 气体传感器 TGS5042 处于工作状态时的电流消耗为 4mA，该状态是传感器节点功耗最大的部分。传感器节点工作在空闲模式时可以切断电源。这种基本方式需要在传感器的电源线上安装可控开关。如图 3.7 所示，在传感器处于空闲模式时，CO 气体传感器电路中的 P 沟道开关晶体管 J177 用来关闭 CO 气体传感器。CO 气体传感器为空闲模式时，微处理器的控制信号将 CO 气体传感器电路断开，因此消耗电流在该状态下为零。CO 传感器在没有使用 P 沟道开关晶体管时一个周期内能耗为 2 640 000μC，而采用 P 沟道开关后能耗缩减为 240 000μC。

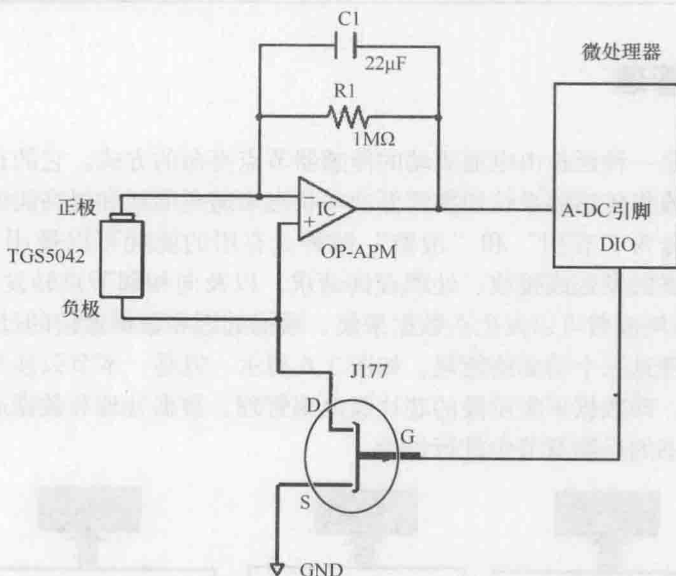


图 3.7 具有 P 沟道开关的 CO 气体传感器

3.6 能量捕获

能量捕获，也叫做能量收集，是另一种延长传感器节点寿命的方法。大多数人还没有意识到，环境中蕴含着丰富的能量，如太阳能、热能、风能和无线频率能

量。如果这些能量可以收集并转换成电能，则可用来为无线设备供电，而先前WSN中电池的重要局限性可以得到解决。根据传感器的不同及传感器所处的不同环境，可以采用不同的能量捕获方式，主要包括以下几种：

- 光能，太阳光或人造光，可以通过太阳能集热板、光敏器件收集。
- 热梯度能量，从加热器、熔炉和发动机等浪费掉的热能。
- 无线电频率能量，来自卫星、电视基站、移动电话传送站和其他无线电子设备。
- 机械能，振动、机械压力、拉力和风能。
- 人体，通过生物有机体或身体动作产生的能量组合。
- 其他能源，化学和生物资源。

常用能量捕获源的功率密度见表3.8（Roundy，2003）。最方便的能源是太阳能，这可以通过光电池转换采集，比其他方式具有较高的功率密度。因此，本节选择太阳能采集系统为例，来说明如何设计补充电池能量的能量捕获系统，以延长WSN的寿命。

表3.8　常用能量捕获源的功率密度

能　量　源	1年寿命，功率密度/($\mu W/cm^3$)
太阳能（户外）	15000（直射光） 150（阴天）
太阳能（室内）	6（办公桌）
振动	200
噪声	0.003（75dB） 0.96（100dB）
每日温度变化	10
温度梯度	15（10K梯度）
鞋垫挤压机械能	330

太阳能是自然光最重要的来源，并且用之不竭。光伏（Photovoltaic，PV）技术是直接将太阳能转换成电能。实际中，通常利用太阳电池收集太阳能。图3.8给出了太阳能能量捕获系统功能框图，包括三个子系统：能量捕获单元、最大功率点跟踪（Maxium Power Point Tracking，MPPT）单元，以及一个电源管理单元。

3.6.1　太阳能捕获单元

太阳电池通常通过收集光照强度来发电。有许多类型的商用太阳电池可以使用。考虑到价格、尺寸和太阳电池的效率，使用两个并联连接的Centennial Solar MC-zSP0.8-NF-GCS（Multicomp，2010）作为能量捕获单元的主太阳电池板，因为一个太阳电池就足以为整个传感节点供电。

3.6.2 最大功率点跟踪单元

MPPT 的主要功能是从太阳电池板向蓄电池发送最大功率。MPPT 单元由一个脉宽度调制（Pulse Width Modulation，PWM）、DC-DC 转换器及 MPPT 外围电路组成。

因为太阳能随光照强度的变化而变化，所以需要一个具有高功率转换效率的能量捕获接口电路将捕获的能量在存储到蓄电池之前进行平滑转换。采用的 DC-DC 转换器的类型由功率捕获强度和蓄电池工作电压共同决定。这里选择的是 LTC3401（Linear Technology，2001）型 DC-DC 转换器，因为它的转换效率超过 85%，输出电流范围为 10 ~ 50 mA，而其输出电压只需设置为 4.1 V（Park 和 Chou，2006）。由于使用 PWM DC-DC 转换器不用通过将二极管与太阳电池直接连接的方式向蓄电池充电，所以 PWM DC-DC 转换器具有两个优点。首先，此 PWM DC-DC 转换器可以使能量捕获持续进行，即使太阳电池的开路电压低于蓄电池的电压。其次，使用二极管来阻止蓄电池的反向电流流向太阳电池，会导致输出电压有 0.7V 的电压降，但是 PWM DC-DC 转换器可避免这种电压降的产生。

MPPT 外围电路由一个小型光伏组件和一个比较器组成。当小型光伏组件和主太阳电池同处于相同的光照下，小型光伏组件的开路电压与太阳电池的最大功率点存在线性关系。鉴于以上的线性关系，可以利用比较器比较主太阳电池的输入和小型光伏组件的反馈来实现 MPPT 功能。这里，选择 Hamamatsu S1087（Hamamatsu，2002）作为小型光伏组件，并将其作为光传感器。该光传感器没有必要使用任何额外的电源。

3.6.3 电源管理单元

电源管理单元，用于能量捕获并确保其有效利用。如图 3.8 所示，电源管理单元由主缓冲区、辅助缓冲区和充电控制电路组成。电源管理子系统使用多个缓冲器有两个原因。随着环境中光照强度的变化，产生的电压也会随时间而变化，因此能量捕获单元很难向目标系统直接供电。因此，必须采用可充电电池这样的高密度能量存储元件积聚由能量捕获单元提供的可用能量。另一方面，可充电电池具有有限的充电周期和寿命，从而限制了整个系统的寿命。为了尽可能延长系统的寿命，对充电电池的访问必须被最小化，因此能量捕获设备应在大部分时间里能直接向目标系统供电。因此，需要另一能量缓冲区。这里的双缓冲设计与 Prometheus 平台的设计思路相同（Jiang 和 Polastre，2005）。主缓冲区，即一个超级电容器，直接由能量捕获板充电，当能量充足情况下为目标系统充电。否则，目标系统从辅助缓冲区，即一个可充电电池，获取电流。此外，如果有足够的光源可用，主缓冲区向辅助缓冲区充电，并同时为目标系统供电。

主缓冲区是由能量捕获单元直接充电。其主要目的是为了尽可能使用减少辅缓

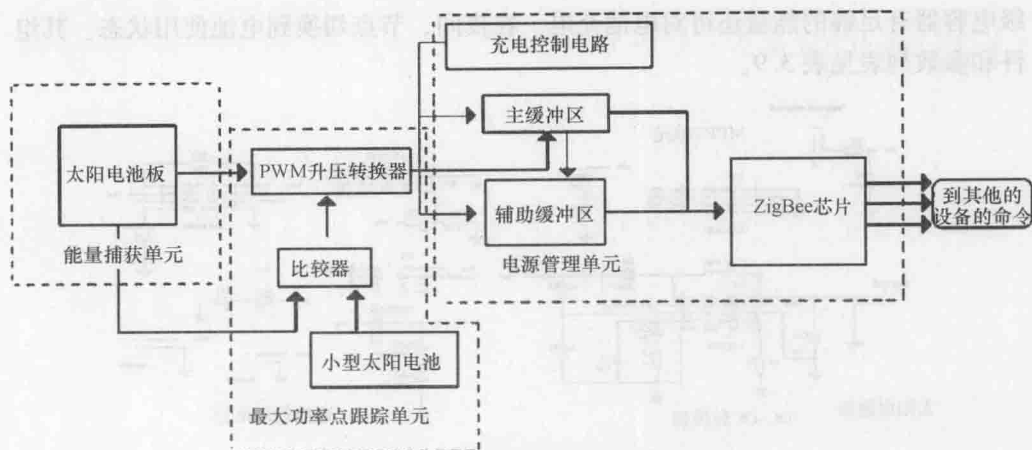


图3.8 太阳能能量捕获系统功能框图（Lu和Yang，2009）

冲区，以延长整个能量捕获系统的寿命。主缓冲区必须能够处理高能量通量和频繁的充电次数，但并不需要长时间保存能量的能力。基本上，超级电容器比可充电电池具有更长的寿命、更高的效率、更高的功率密度及简单的充电电路。这意味着超级电容器满足所有主缓冲区的要求。因此，在本设计中选择两个22F超级电容器作为主缓冲区。

只有当主缓冲区中的能量耗尽时或需要长时间保持能量（即具有较低的泄漏电流）时，才使用辅缓冲区。可充电电池具有更高的能量密度、较低的击穿电压和较低的泄漏电流。由于这些原因，可充电电池是辅助缓冲的理想选择。

充电控制电路用来优化传感器节点对能量捕获的利用。采用Ambimax架构设计（Park和Chou，2006）作为充电控制电路。通过比较超级电容器的两端电压与预定义的阈值电压，充电控制电路在任意时刻都可以决定是选择主缓冲区还是辅助缓冲区为目标系统供电。当充电电池不能完全充电并且超级电容器的电压高于第二预定义阈值电压，充电电池将由超级电容器充电。另外，充电电池由安装在ZigBee芯片的软件进行保护，防止其充电过量或充电不足。

3.6.4 设计案例

太阳能能量捕获系统的完整电路如图3.9所示。在图中，太阳电池板与DC-DC转换器电路位于左下方，用于从环境中收集太阳能；左上方的MPPT电路用来保持太阳电池以最大功率点工作；右方是电源管理电路，用于最大化系统的寿命。它由一个LTC1441双比较器、充电控制芯片MAX890L、两个22F超级电容器及两个充电电池组成。温度传感器和CO气体传感器ZigBee节点与太阳能捕获系统相连。整个系统在室外环境中进行了为期一周的测试。传感器节点在不需要任何额外功率的情况下如期自主工作。在白天，该传感节点大部分时间由超级电容器供电，如果超

级电容器有足够的能量还可对电池充电。在夜间，节点切换到电池使用状态。其组件和参数列表见表 3. 9。

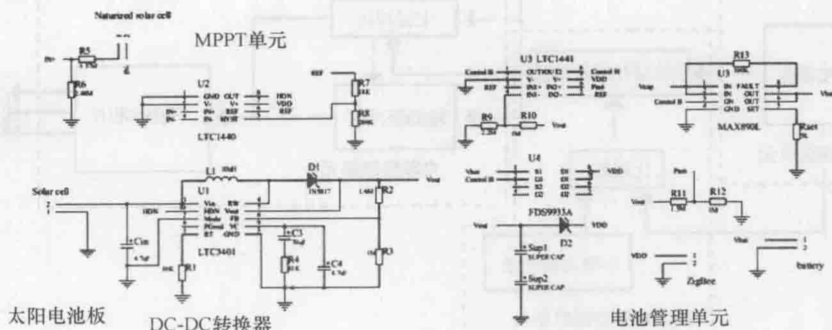


图 3. 9　太阳能能量捕获系统的完整电路

表 3. 9　组件和参数列表

编　号	说　明
Buttery	充电电池
C3	电容 70μF
C4	电容 4. 7μF
Cin	电容 4. 7μF
D1	二极管 1N5817
D2	二极管 1N5817
L1	电感 CDR，10μH
Naturized solar cell	小尺寸太阳电池
R1	电阻 10kΩ
R2	电阻 1. 6MΩ
R3	电阻 1MΩ
R4	电阻 81kΩ
R5	电阻 1. 37MΩ
R6	电阻 2. 48MΩ
R7	电阻 18kΩ
R8	电阻 200kΩ
R9	电阻 2. 2MΩ
R10	电阻 1MΩ
R11	电阻 1. 5MΩ

(续)

编 号	说 明
R12	电阻 1MΩ
R13	电阻 100kΩ
Rset	电阻 5kΩ
Solar cell	太阳电池
Sup1	22F 超级电容
Sup2	22F 超级电容
U1	LTC 3401 DC-DC 转换器
U2	LTC 1440 比较器
U3	LTC 1441 双通道比较器
U4	MAX890L 充电控制芯片
ZigBee	Jennic 传感器电路板

3.7 小结

硬件设计是 WSN 中最关键的步骤之一，而能耗是其中最重要的方面。本章将传感器节点的基本结构分为传感部分、微处理器部分、RF 收发模块和电源部分。许多无线电子产品制造商提供集成微处理器、RF 收发器及外围电路的电路板，即之前讨论的 SoC 解决方案。基于 SoC 的传感器节点设计方案比基于组件的设计方案更快、更容易，而且更加可靠。本章总结了在微处理器和通信设备选择及传感器设备和电源设备设计时需考虑的各种因素，并阐述了在温度传感器和 CO 气体传感器节点设计时如何进行使用。电源管理和能量捕获这两种方法用来克服能耗的限制，并延长传感器网络的寿命。当传感器节点休眠时，关闭电源可以降低能耗。本章设计了完整的太阳能捕获系统，表明了未来该类技术在 WSN 方面的发展前景。

参考文献

Cook, D.J., Das, S.K.: Smart Environments: Technology, protocols and Applications. Wiley, London (2004)

Dallas Semiconductor: Maxim DS18B20 programmable resolution 1-wire digital thermometer. Available at http://datasheets.maxim-ic.com/en/ds/DS18B20.pdf (2008)

Figaro: TGS 5042. Available at http://www.figaro.co.jp/en/data/pdf/20101202115721_7.pdf (2010)

Hamamatsu: S1087 photodiode, 56NM, Ceramic, Max voltage 10 V. Available at http://www.farnell.com/datasheets/104399.pdf (2002)

Jennic: JN5139 Module datasheet, http://www.jennic.com/files/product_briefs/JN5139-xxx-Myy-PB_v1.2.pdf (2010)

Jiang, X., Polastre, J., and Culler, D.: Perpetual environmentally powered sensor networks, Information Processing in Sensor Networks, IPSN, pp. 463–468 (2005)

Linear Technology: LTC3401 1A, 3 MHz micropower synchronous boost converter. Available at http://cds.linear.com/docs/Datasheet/3401fb.pdf (2001)

Lu, X., Yang, S.H.: Solar energy harvesting for ZigBee electronics, Sustainability in energy and buildings, pp. 19–27 (2009). doi: 10.1007/978-3-642-03454-1

Multicomp: MC-SP0.8-NF-GCS Solar panel. Available at http://www.farnell.com/datasheets/925851.pdf (2010)

Park, C., Chou, P.H.: AmbiMax: autonomous energy harvesting platform for multi-supply wireless sensor nodes, IEEE SECON 2006 Proceeding, pp. 168–177 (2006)

Ristic, L.: Sensor Technology and Devices. Artech House, London (1994)

Roundy, S.J.: Energy scavenging for wireless sensor nodes with a focus on vibration to electricity conversion. Internal report of Engineering-Mechanical Engineering in the Graduate Division of The University of California, Berkeley (2003)

Swanson, C.: Sensor Selection Guide, Watlow Electric Manufacturing Company. Available at http://www.newark.com/pdfs/techarticles/Accurate_Temperature_Measurement-Sensors.pdf (2010)

第 4 章　无线传感器网络的嵌入式软件设计

关键词： 传感器驱动程序　网络构建　网络管理　嵌入式软件设计　IEEE 802.15.4　ZigBee

4.1　引言

在 WSN 的设计与开发过程中，嵌入式软件设计是最重要的，也是很困难的任务。这里的“嵌入式”的准确含义是“内置”的意思。嵌入式系统无处不在，典型的例子有移动电话、微波炉、数码相机等。嵌入式软件是一种计算机软件，它在装配该软件的电子设备中发挥着不可或缺的作用。通常嵌入式软件是为专用微处理器编写的，这种处理器具有低计算能力、低成本、有限内存和低功耗的特点。嵌入式软件通常是运行在实时操作系统（Real-Time Operating System，RTOS）（Laplante，2004）中，嵌入式系统所使用的通信协议是来自微处理器制造商的闭源代码。在设计完成后，嵌入式软件必须上传到相应的微处理器上，而且能够在其上进行验证和运行，并集成在电子设备中。理论上，嵌入式软件的设计要在相关的硬件设计完成后才能进行。然而随着大量嵌入式软件仿真环境的发展，嵌入式软件设计可以和硬件设计同时进行，甚至可以提前进行。COOJA（http://www.contiki-os.org/start.html）就是这样的一个仿真软件。COOJA 是一个基于 Contiki 操作系统的 WSN 仿真软件，在这个环境中，嵌入式软件设计就可以同时与硬件设计进行，甚至提前进行。

嵌入式软件和与其相匹配的硬件就构成了一个专用的嵌入式系统。图 4.1 给出了嵌入式系统的设计过程。首先是系统需求，接着是系统体系结构的设计和微处理器的选择，然后是同时进行软件设计和硬件设计，最后进行软件和硬件的集成（Labrosse 等，2008）。

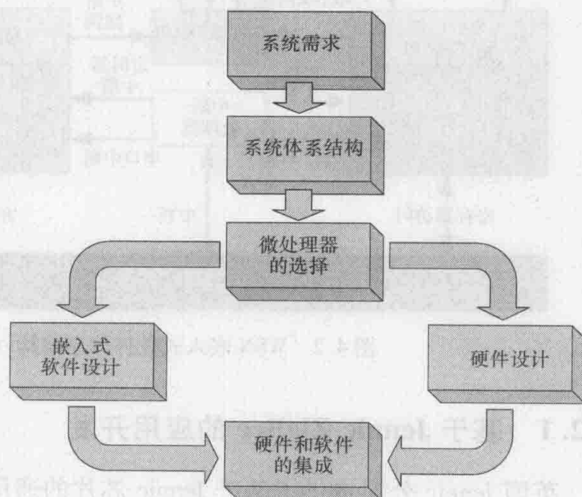


图 4.1　嵌入式软件系统的设计过程

4.2 无线传感器网络的嵌入式软件设计

根据嵌入式系统中使用的微处理器和通信协议，嵌入式软件的体系结构因系统而异。WSN 协议栈在本书第 2 章已给出（见图 2. 2），该协议栈也构成了 WSN 的软件体系结构。为简单起见，图 2. 2 所示的协议栈由四层组成，自下而上分别是硬件层、MAC 层、网络层和应用层。图 4. 2 给出了 WSN 嵌入式软件体系结构（Jennic，2010）。应用程序位于 IEEE 802. 15. 4 协议栈之上，而 IEEE 802. 15. 4 协议栈位于基带硬件之上。IEEE 802. 15. 4 协议栈具有预定义的接入点，如请求 IEEE 802. 15. 4 动作、初始化和注册回调应用。应用队列应用编程接口（Application Programming Interface，API）、集成外设 API 和板卡 API，它们在逻辑上位于 IEEE 802. 15. 4 协议栈上，但又独立于 IEEE 802. 15. 4 协议栈。像通信、传感器访问、系统控制和任务调度这样的操作可以通过调用 API 来实现。换句话说，用户应用是由一系列基于这些 API 的调用组成的。如图 4. 2 所示，通信服务是通过调用 IEEE 802. 15. 4 协议栈 API 来实现的；传感器访问和本地 PC 的连接是通过调用集成外设 API 来完成的；硬件中断是通过调用应用队列 API 产生的。板卡 API 用于工具箱的开发。因此，在大多数应用中，基于 WSN 的嵌入式软件设计就变成了通过使用 API 来完成任务的过程。

应用
MCPS 请求/确认
MLME 请求/确认
MCPS/ MLME回调
队列轮询 请求/响应
硬件 中断 回调
命令/响应
命令/响应
802.15.4 协议栈API
应用队列API
集成外设API
命令
板卡API
PHY 中断
定时器 中断
IEEE 802.15.4 协议栈层
中断 处理器
外围硬件 驱动器
基带中断
串口中断
寄存器访问
中断
寄存器访问
硬件

图 4. 2 WSN 嵌入式软件体系结构（Jennic，2010）

4.2.1 基于 Jennic ZigBee 的应用开发

英国 Jennic 公司提供了基于 Jennic 芯片的通用 ZigBee 嵌入式软件结构，如图 4. 3 所示。它提供了 10 个预定义的功能，如用户任务和 BOS/Stack 任务。后者为不需要用户干预的基本操作系统（Basic Operating System，BOS）任务。嵌入式软

件开发任务就是实现这10个预定义的功能。

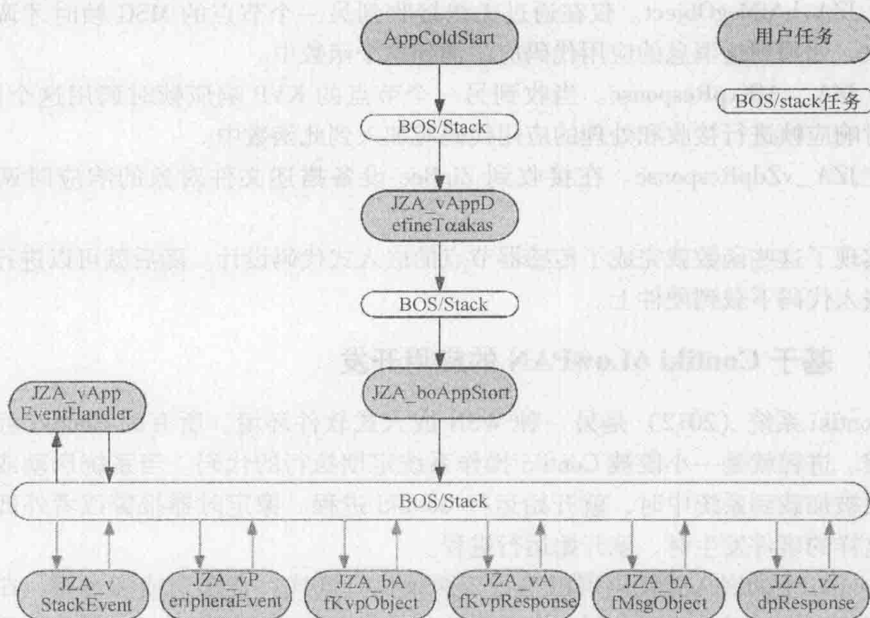


图4.3 通用ZigBee嵌入式软件结构（Jennic，2008b）

当传感器节点上电时，程序开始执行“AppColdStart”函数，此时系统被初始化。任何用户变量或系统外设，如定时器或UART端口，都会在这个函数里被初始化。此外，必要的ZigBee系统参数，如无线信道和网络识别，也在这个函数中进行配置，从而使传感器节点加入到恰当的WSN中。最后，BOS进行初始化并启动，使传感器节点处理硬件事件。系统初始化后，BOS在调用函数“JZA_vAppDefine-Tasks”之前先执行一些内部函数，此时用户应用可以进行额外任务的注册。通过执行另一个初始化函数“JZA_boAppStart”，注册的ZigBee设备通过调用“ZigBee stack”可以充当ZigBee协调器、路由器或终端设备进行运行。

在BOS和ZigBee栈启动后，BOS将通过下面的函数向用户应用传递控制：

● JZA_vAppEventHander。这是个被BOS定期调用的用户应用函数。任何需要定期执行的用户应用代码都放在这里。

● JZA_vStackEvent。调用这个函数来处理来自低层协议栈的各种事件。

● JZA_vPeripheralEvent。当系统外设产生中断时调用这个函数，如一个定时器报警或DIO线被中断。当处理器正运行于中断模式时调用这个函数。有关中断的信息记录在一个简单的FIFO队列中，等待JZA_vAppEventHandler（ ）函数读取。

● JZA_bAfKvpObject。只有当通过无线接收到另一个节点的键值对（KVP）命令帧时才调用这个函数。用来处理到达的命令的应用代码将添加到这个函数中，并

且如果有必要会产生响应。

- JZA_bAfMsgObject。仅在通过无线接收到另一个节点的 MSG 帧时才调用这个函数。处理到达消息的应用代码应添加到这个函数中。
- JZA_vAfKvpResponse。当收到另一个节点的 KVP 响应帧时调用这个函数。用来对响应帧进行接收和处理的应用代码应加入到此函数中。
- JZA_vZdpResponse。在接收到 ZigBee 设备描述文件对象的响应时调用此函数。

实现了这些函数就完成了传感器节点的嵌入式代码设计。随后就可以进行编译和将嵌入代码下载到硬件上。

4.2.2 基于 Contiki 6LowPAN 的应用开发

Contiki 系统（2012）是另一种 WSN 嵌入式软件环境。所有的 Contiki 程序叫做进程。进程就是一小段被 Contiki 操作系统定期执行的代码。当系统启动或者进程模块被加载到系统中时，就开始运行 Contiki 进程。像定时器报警或者外部事件触发这样的事件发生时，就开始运行进程。

Contiki 中的嵌入式代码可以运行于两种执行模式：合作型或强占型。在合作型执行模式中运行的代码与同一模式下的其他代码是顺序运行的。其他合作型的调度代码必须在合作型代码结束后才能运行。强占型代码可以在任何时间中断合作型代码。当强占型代码中断合作型代码时，合作型代码只有在中断型代码执行结束后才能继续。Contiki 中两种执行模式的关系如图 4.4 所示。进程总是在合作型模式中运行。强占模式可以用于设备驱动程序中的中断处理程序和具有指定时限的实时任务调度。

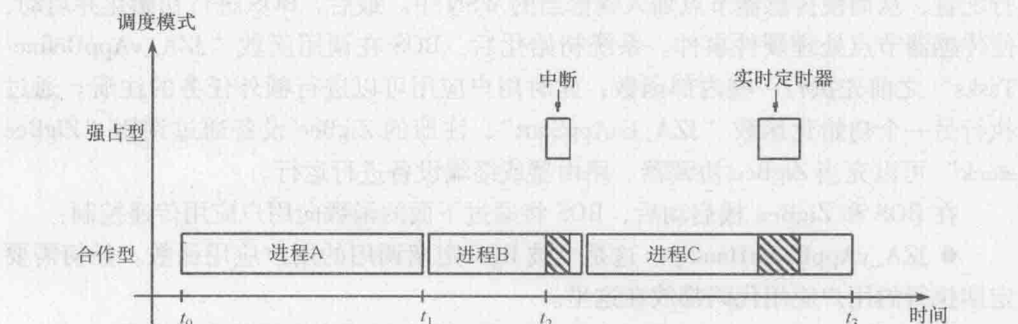


图 4.4 Contiki 中两种执行模式的关系

Contiki 进程由两部分组成：进程控制块和进程线程。进程控制块存储在 RAM 中，包含进程的运行信息，如进程的名字、进程的状态和进程线程指针。进程控制块很小，只需两个字节的内存。进程线程是进程的代码，存储在 ROM 中。

进程控制块不用直接声明或定义，而是通过宏 PROCESS（ ）就可以使用。这

个宏有两个参数：访问进程时使用的进程控制块的变量名，以及调试和向用户输出活动进程列表时使用的进程文本名。例如，Hello World 的进程控制块的定义如下：

```
PROCESS(hello_world_process, "Hello world process");
```

如前所述，进程线程包含进程的代码。进程线程是由进程调度器产生的单个原始线程。例如：

```
PROCESS_THREAD(hello_world_process, ev, data)
{
  PROCESS_BEGIN();
  printf("Hello, world\n");
  PROCESS_END();
}
```

图 4. 5 给出了通用 Contiki 进程结构，是编写一个 Contiki 工作进程的定义顺序。在进程控制块的定义完成之后，就调用“AUTOSTART_PROCESS”来启动进程。然后进行“PROCESS_THREAD”的定义。通过调用“PROCESS_BEGIN”和“PROCESS_END”来分别启动和终止进程。进程代码就插入到位于“PROCESS_BEGIN”和“PROCESS_END”之间的“WHILE”循环中。“WHILE”循环中也包含了许多特殊函数，如事件等待和事件处理函数。

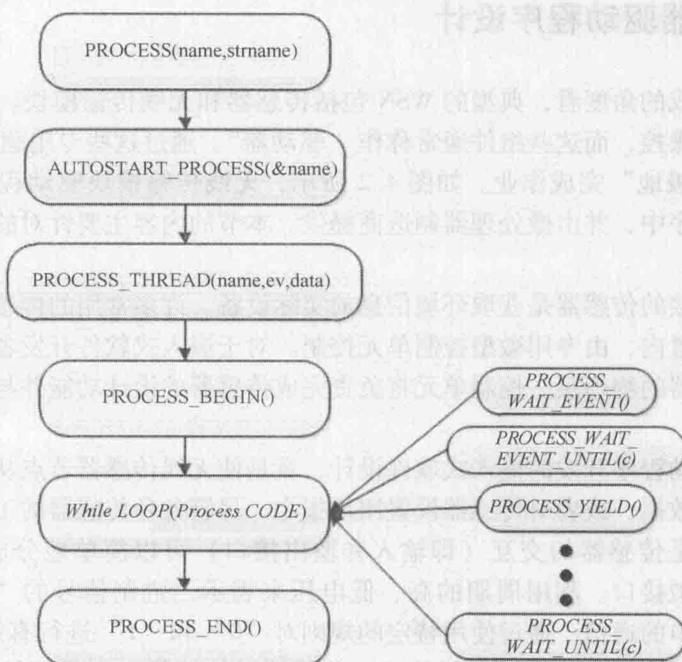


图 4. 5　通用 Contiki 进程结构

下面的例子是用定时器每隔 3s 打印输出一行特定的文本。进程的名字叫“example_ process”。通过执行定时器结构体“etimer”来生成定时器事件“PROCESS_EVENT_TIMER”。在“WHILE”循环中还调用了“PROCESS_WAIT_EVENT_UNTIL”函数。

```
#include "contiki.h"
#include<stdio.h>
PROCESS(example_process, "Example process");
AUTOSTART_PROCESSES(&example_process);
PROCESS_THREAD(example_process, ev, data){
static struct etimer timer;
PROCESS_BEGIN();

  etimer_set(&timer, CLOCK_CONF_SECOND*3);
  while(1){

PROCESS_WAIT_EVENT_UNTIL(ev == PROCESS_EVENT_TIMER);
printf("Hello Mr. Yang To Saudi Arabia\r\n");
etimer_reset(&timer);
  }
PROCESS_END();
}
```

4.3 传感器驱动程序设计

从硬件组成的角度看，典型的 WSN 包括传感器和无线传输模块。这些组件需要嵌入式软件操控，而这些组件通常称作“驱动器”。通过这些专用驱动器，“哑”硬件可以“积极地”完成作业。如图 4.2 所示，无线传输模块驱动程序包含在外围硬件驱动程序中，并由微处理器制造商提供。本节的内容主要针对的是传感器驱动程序的开发。

网络中连接的传感器是获取环境信息的实际设备。许多常用的传感器都被封装在一个微型装置内，由专用微型控制单元控制。对于嵌入式软件开发者来说，没有必要访问传感器的物理层。控制单元将负责完成传感器的设计功能并与外部控制系统进行交互。

传感器驱动程序开发的嵌入式软件设计，就是使无线传感器节点从预定的传感器获取传感器数据，或者对传感器设置用户指令。尽管各种传感器的工作原理可能完全不同，但是传感器的交互（即输入和输出接口）可以简单地分成两种形式：数字接口和模拟接口。利用周期的高、低电压来表示二进制信号的“1”和“0”来完成数字接口的通信。通过使用特定的规则对“0”和“1”进行有意义的整合，开发者可以发送与接收传感器控制单元（传感器微处理器）和外部控制系统（无线芯片）都兼容的信息。图 4.6 给出了数字传感器的通用结构。通过数字接口、

内部的 A-DC 在微处理器的作用下输出数字信号。有许多可用于构建数字接口的数字通信标准（即通信规则），如串口通信协议、SMBus[1]协议（美国 Intel 公司定义)、I^2C[2]协议（曾由荷兰 Philips 半导体公司定义，但是现在属于荷兰 NXP 半导体公司)、通用异步接收器/发送器（Universal Asynchronous Receiver/Transmitter，UART)、单总线接口（由美国 Maxim 集成产品公司定义）等。

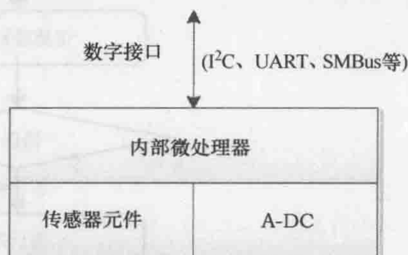


图 4.6　数字传感器的通用结构

与数字接口相比，模拟通信接口更简单些。通常模拟传感器输出与感测现象的变化相应的电压值。A-DC 将电压值转换成数字信号形式后，外部控制系统就可以使用该电压值了。某些模拟传感器的输出由发送的一系列的脉冲组成，这些脉冲与外部控制器感测的现象（声音、光、温度等）强度有关。外部控制系统以一定周期对脉冲进行采样后，按照预定公式转换成有意义的数值，最后呈现给用户。

4.3.1　传感器驱动程序设计一般步骤

传感器驱动程序应该向外部控制器提供获取传感器读数和将用户指令传送给传感器的能力。一般的，一个完整的传感器驱动程序设计由传感器初始化、传感器参数设置、传感器数据采集、传感器电源管理（休眠、等待、待机）等步骤组成。图 4.7 给出了传感器驱动程序设计通用流程图。

下面将更详细地描述这些过程：

传感器初始化。第一步是“传感器初始化”，负责初始化所有默认的传感器参数。这步涉及的各个阶段包括传感器上电、设置通信接口、传感器默认参数恢复。许多传感器将这些参数设置存储到已连接的非易失性存储器中，例如，电可擦除只读存储器（Erasable Programmable Read-Only Memory，EEPROM)。将用户配置参数或者指定的生产商参数存储在非易失性存储器中，这非常安全且易于恢复。

错误报告。在启动期间，传感器可能没有正确响应，这意味着发生了某种错误。为了保证外部控制系统免受传感器故障的影响，这个阶段必须具有相应的错误处理过程。

用户指令。在传感器成功初始化之后，驱动程序将准备执行用户指令。在工作周期结束之前，传感器驱动程序处于的五个阶段为，读取传感器、待机、休眠、唤

[1] SMBus：System Management Bus，系统管理总线。
[2] I^2C：Inter-Integrated Circuit，内部集成电路。

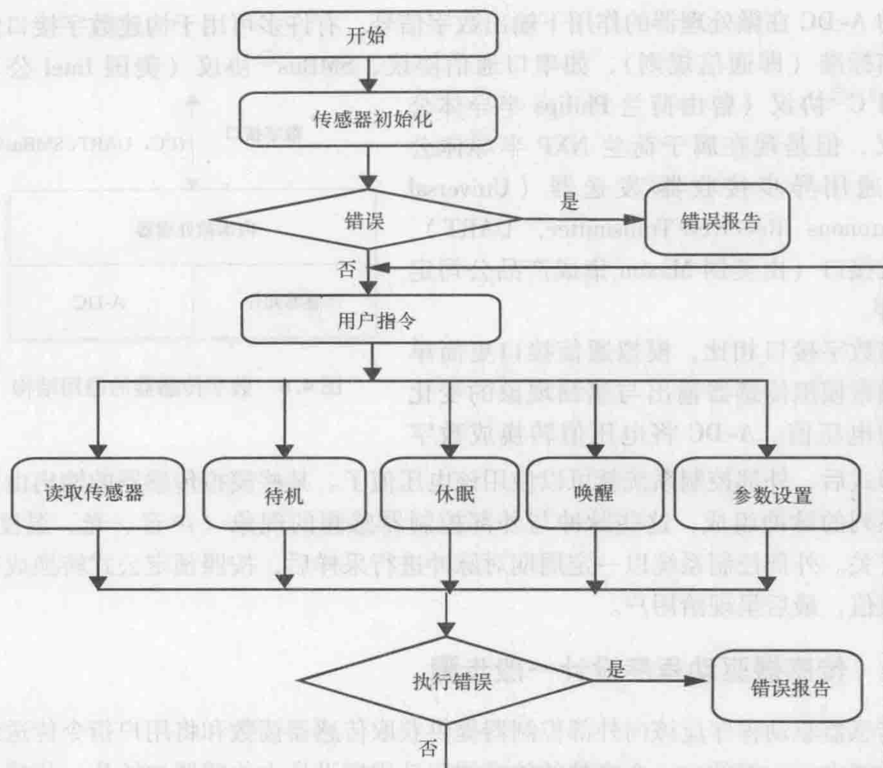


图 4.7　传感器驱动程序设计通用流程图

醒和参数设置。传感器的特性和使用范围依赖应用需求。对于所有的传感器驱动程序设计，不可能给出一个统一详细描述。但是，上述这五个阶段是基本的组成部分，任何传感器的使用都应包含这几个阶段。

a）读取传感器。在传感器驱动程序设计中，"读取传感器"是最重要的功能。为了获取传感器数据，外部控制器发送请求指令来启动读取程序。在读取程序完成时，传感器数据就可用来输出。因为传感器的材质不同，许多传感器（温度传感器、振动传感器、湿度传感器等）执行测量任务需要花费一些时间，即采样周期。驱动程序等待传感器的输出有两种处理方法：一种方法是驱动程序独占通信接口直到采样周期结束，如图 4.8 所示；另一种方法是使用硬件中断，驱动程序在发送数据请求命令之后就释放通信接口，而当采样结束之后再占用通信接口，如图 4.9 所示。第一种方法可以确保驱动程序的编程连贯性，这意味着函数可以返回期望的结果。但是这种方法有缺点，在等待传感器数据的同时，驱动程序一直占用处理器线程，而不是将处理器线程返还给系统，从而使其他普通的任务也可能被中断。如果外部控制系统的处理器同时也是无线通信模块的控制器，就会产生非常严重的后果。为了避免控制系统的介入，可以考虑采用第二种方法。传感器驱动程序可以要

求外部控制器设置中断，而当传感器已经完成采样任务并准备输出结果时，就触发中断。一收到中断，外部控制器就开始读取传感器。随后，系统就可以处理其他任务。第二种方法的缺点是增加了系统开销。因为采样周期完成的指示需要控制器的协助，传感器驱动程序不能独立于系统。如果选择的控制器发生了变化，那么传感器驱动程序也需要进行更改。

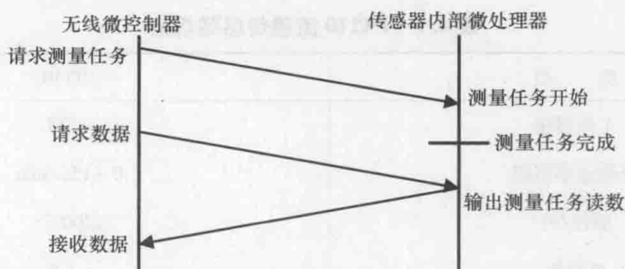


图 4.8　独占接口传感器读取数值请求方法

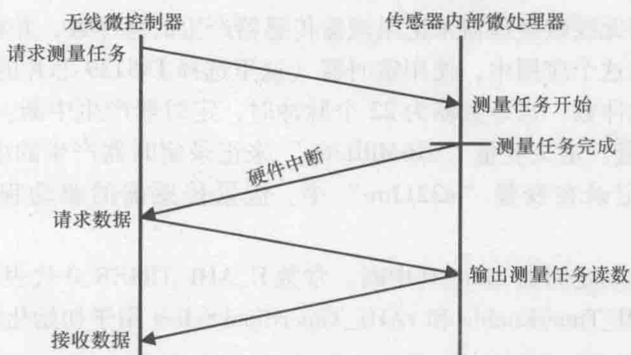


图 4.9　基于硬件中断的传感器读取数值请求方法

b）待机、休眠、唤醒。通常，WSN 使用的资源是极其有限的。并且，电源管理对于延长系统的寿命是非常重要的。因为传感器的特性不同，所以电源管理的实际规范视不同情况而定。一般来说，驱动程序设计必须包含这三种功能（待机、休眠、唤醒）。只要没有测量任务，传感器应尽可能处于休眠状态。但是，在某些情况下，如频繁地读取传感器数据，如果从休眠模式唤醒传感器的过程比在正常状态（某些电化学的传感器需要一定的时间来重建稳定状态）下消耗的能量还多，那么可以让传感器最好处于待机状态。在电源管理模块的设计过程中，仔细计算能耗是首要的。

c）参数设置。如果传感器配置可调的话，传感器驱动程序应允许应用（即用户）根据需要来改变参数。

d）执行错误。如果用户指令执行失败，设计应该监控指令执行的返回错误并

将其放到相应的错误处理函数中。这些函数是保持系统稳定的有效措施。

4.3.2　模拟流量传感器驱动程序设计

本节用 FT110 流量传感器（Gems Sensors，2008）来阐述如何设计和编写基于硬件中断的模拟传感器的驱动程序。FT110 流量传感器的规范见表 4.1。

表 4.1　FT110 流量传感器规范

类　　型	FT110
工作温度	-20℃
流量速率范围	0～15L/min
脉冲/升	2200 个
准确度	±3 %

根据表 4.1，FT110 流量传感器每升产生 2200 个脉冲。因此，流量传感器的驱动程序可以使用无线微处理器来记录流量传感器产生的脉冲数，并将该脉冲数转换成流量速率。在这个应用中，使用定时器（这里选择 JN5139 芯片的 Timer 0）的捕获函数来计算脉冲数。当计数器为 22 个脉冲时，定时器产生中断。22 个脉冲表明 10mL 水的使用量。定义变量“u16MillLitre”来记录定时器产生的中断次数。最终的流量测量值记录在变量“u32Litre”中。流量传感器的驱动程序由以下三步组成：

第一步，启动定时器 Timer 0 中断。常数 E_AHI_TIMER_0 代表定时器 Timer 0. 预定义函数 vAHI_TimerEnable 和 vAHI_TimerClockSelect 用于初始化定时器。

```
vAHI_TimerEnable(E_AHI_TIMER_0,

    0,
    FALSE,
    TRUE,
    FALSE);
vAHI_TimerClockSelect(E_AHI_TIMER_0, TRUE, FALSE);
```

第二步，为定时器 Timer 0 设置数值。当 Timer 0 计数到 22 个 FT110 传感器脉冲时，产生中断。使用预定义函数 vAHI_TimerStartRepeat 设置定时器数值并产生中断。

```
vAHI_TimerStartRepeat(E_AHI_TIMER_0,

    0x0000,
    22); //number 22 is set for FT110 sensor
```

第三步，处理流量传感器读数。当 JN5139 芯片检测到 Timer 0 产生的中断时，JN5139 处理流量传感器的读数。常数 E_AHI_DEVICE_TIMER0 表示 JN5139 无线微处理器接收到中断。

```
case E_AHI_DEVICE_TIMER0:
  vProcessFlowMeter();
PRIVATE void vProcessFlowMeter(void)
{
/*water usage reading increase by 1 (Milliliter) when an interruption is detected. */
/*Every 100 interruptions. u32Liter increase by 1 (liter) and u16MillLitre = 0*/
  u16MillLitre++;
  if(u16MillLitre == 100)
  {
u32Litre++;
u16MillLitre = 0;
  }
}
```

4.3.3　数字温度传感器驱动程序设计

选择 Maxim DS18B20（Maxim，2009）数字温度传感器作为例子来阐述数字传感器驱动程序的设计。DS18B20 传感器是典型的低功耗数字传感器。由于它具有低电压（直流 3.0～5.5V）和宽测量范围（－55～＋25℃）的特点，因而适用于许多应用情况。DS18B20 传感器的所有操作仅需一个 1-Wire 型接口就可完成。图 4.10给出了 DS18B20 传感器与外部微处理器之间的连接示意图。温度传感器与外部微处理器（这里选择 JN5139 芯片）通过 1-Wire 型接口进行通信，这里将外部微处理器定义为主设备，而将 DS18B20 传感器定义为从设备。

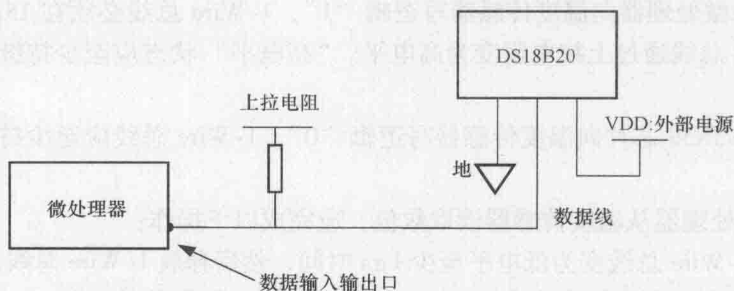


图 4.10　DS18B20 传感器与外部微处理器之间的连接示意图

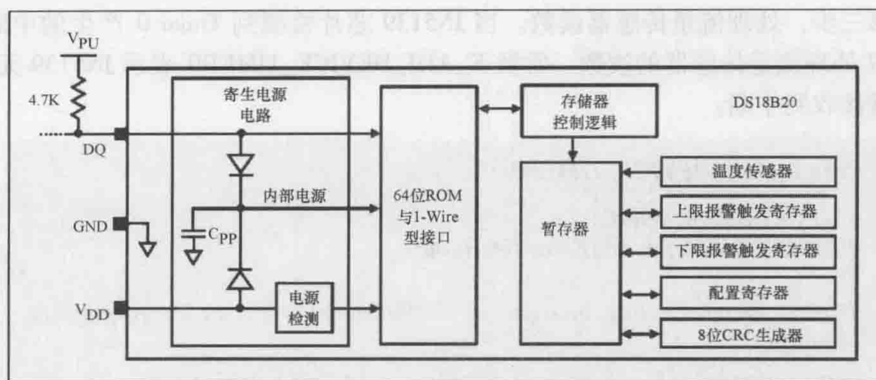


图 4.11　DS18B20 传感器的框图

图 4.11 给出了 DS18B20 传感器的框图。“64 位 ROM 与 1-Wire 型接口”和“暂存器”是传感器驱动程序需要使用的两个存储空间。64 位传感器标识符和 1-Wire型接口协议驻留在“64 位 ROM 与 1-Wire 型接口”中，为用户进行配置的存储映射由暂存器提供。暂存器由 9 个字节组成，包含多个参数。例如，暂存器的第 1、2 字节存储的是传感器读取值；第 3、4 字节分别为测量值的上限和下限；第 5 ~7 字节预留给其他用途，如设置分辨率；最后一个字节是 CRC 校验值。图 4.11 也给出了暂存器与温度传感器、报警寄存器、配置寄存器及 CRC 生成器之间的连接。

从图 4.7 可以看出，传感器驱动程序的核心操作是传感器初始化、参数设置、从传感器读取数值、向传感器写命令，如使传感器进入待机、休眠、唤醒模式。图 4.12给出了 DS18B20 传感器读/写时隙时序图。图中从左到右从上到下显示了主设备（这里以 JN5139 为例）写逻辑“0”、“1”和读逻辑“0”、“1”的过程。传感器通过改变自己的逻辑状态来满足主设备的操作需求。

更详细地说，当微控制器发出一个写操作时，应完成以下操作：

1. 轮询使 1-Wire 总线为低电平。

2. 如果微处理器向温度传感器写逻辑“1”，1-Wire 总线必须在 15μs 内释放；然后 1-Wire 总线通过上拉电阻变为高电平。“高电平”状态应至少持续 15μs 或者最多 45μs。

3. 如果 JN39 芯片向温度传感器写逻辑“0”，1-Wire 总线应至少持续 60μs 的低电平。

如果微处理器从温度传感器读取数值，应完成以下操作：

1. 将 1-Wire 总线变为低电平至少 1μs 时间，然后释放 1-Wire 总线。

2. DS18B20 传感器开始在 1-Wire 总线上向微处理器传输逻辑“1”或“0”。DS18B20 传感器通过使总线处于高电平来传输“1”，通过使总线处于低电平来传

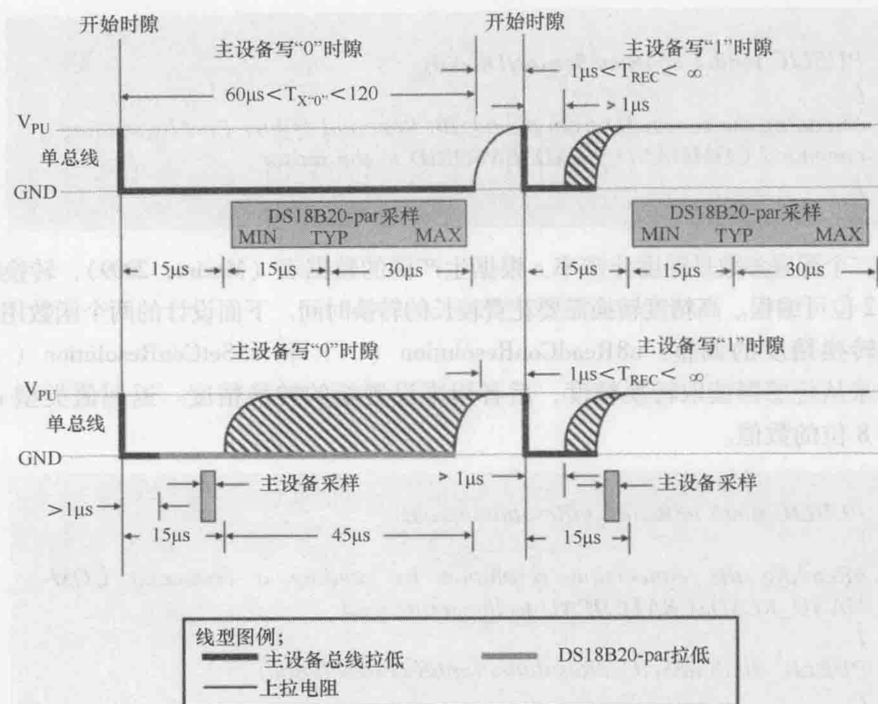


图 4.12　DS18B20 传感器读/写时隙时序图（Maxim，2009）

输"0"。

3. 温度传感器在读取时隙结束后将释放 1-Wire 总线，总线被置为高电平状态。在启动读取时隙的下降沿的 15μs 内，从温度传感器输出的数据是有效的。因此，微处理器必须释放 1-Wire 总线，并且从启动读取时隙 15μs 内对总线进行采样。

在读/写温度传感器之前，应该执行温度传感器的初始化程序。

```
PUBLIC bool_t Init_DS18B20(void)
{
//adding initialization here
}
```

通常，每个 DS18B20 传感器具有一个唯一存储在"64 位 ROM 与 1-Wire 接口"中的 64 位标识符。当多个传感器通过 1-Wire 接口连接在微处理器上时，传感器 ID 可以用来区别各个传感器。当函数 function u64ReadSensorID（　）被调用时，其返回值就是传感器 ID，一个 64 位的数值，即 uint64。

```
PUBLIC uint64 u64ReadSensorID(void)
{
//Reading the sensor ID from the 64_Bit Rom and 1-Wire Port by sending a
command COMMAND_READSENSORID to the sensor
}
```

第二个配置参数是温度分辨率。根据生产商的数据表（Maxim，2009），转换精度为9~12位可编程。高精度转换需要花费较长的转换时间。下面设计的两个函数用来完成温度转换精度的调整：u8ReadConResolution（ ）和 u8SetConResolution（ ）。前者用来从传感器读取转换精度，后者用来设置新的转换精度。返回值类型 uint8 为一个 8 位的数值。

```
PUBLIC uint8 u8ReadConResolution(void)
{
//Reading the conversion resolution by sending a command COM-
MAND_READSCRATCHPAD to the scratchpad
}
PUBLIC uint8 u8SetConResolution(unit8 u8Resolution)
{
//Setting the new conversion resolution by sending a command COM-
MAND_WRITESCRATCHOAD to the scratchpad
}
```

在完成了温度传感器的初始化和配置之后，可以使用两个函数 vStartConversion（ ）和 u16ReadTemperature（ ）来进行温度的读取。启动 DS18B20 传感器进行温度转换。一旦函数被调用，系统必须启动定时器，一段时间后定时结束。这个时间段长度由转换精度决定。

```
PUBLIC void vStartConversion(void)
{
//Starting temperature conversion by sending a pre-defined command
COMMAD_STARTCONVERSION to the scratchpad
}
```

通过调用函数 u16ReadTemperature（ ）可以获取温度读数。在微处理器读取温度读数之前，传感器读数保存在暂存器的第 1、2 字节内。数值的上限和下限保存在暂存器的第 3、4 字节内。读数的有效性由 CRC 生成器调用函数 u8CRCCaculation（ ）来进行校验。

```
PUBLIC uint16 u16ReadTemperature(void)
{
//Obtaining the sensor reading by sending a pre-defined command COM-
MAD_READSCRATCHPAD to the scratchpad
}
PRIVATE uint8 u8CRCCaculation(unit8* content, uint8 u8Length)
{
//validating the return value from the function u16ReadTemperature. The
first parameter is the reading, and the second is the length
}
```

总之，任何数字传感器驱动程序的设计应该遵循以下七个步骤：

1. 初始化传感器。
2. 从传感器读取唯一的传感器 ID。
3. 从传感器读取转换精度。
4. 向传感器设置转换精度。
5. 启动数值转换。
6. 读取传感器数值。
7. CRC 校验。

4.4 基于 IEEE 802.15.4 的无线传感器网络实现

在本书第2章，图2.8 给出了建立 WSN 的一般步骤，一共有七个阶段：（1）无线信道评估；（2）网络初始化；（3）网络构建公告；（4）监听/启动连接申请；（5）监听/启动拆除申请；（6）网络命令传输与接收；（7）用户数据发送/接收。本书2.3 节给出了各个阶段的详细过程。本节将从嵌入式软件设计的角度来描述这个过程的实现。为了方便，这里将图2.8 表述为图4.13。

图4.13 所示的过程同样适用于采用 ZigBee 协议栈或 IEEE 802.15.4 协议栈的实现过程。在这两种情况下，构建 WSN 的过程是相似的。区别在于，为了应用的快速开发，ZigBee 协议栈提供了更便利的管理功能，如多跳路由协议等。由于 ZigBee协议栈位于 IEEE 802.15.4 协议栈之上，本节采用 Jennic IEEE 802.15.4 协议（Jennic 2008a）语法，只给出 ZigBee 协议栈的实现过程。

两个从网络层到 MAC 层的主要函数调用由 MAC 层管理实体（MAC Layer Management Entity，MLME）和 MAC 公共部分子层（MAC Common Part Sublayer，MCPS）构成，其实现过程如下：

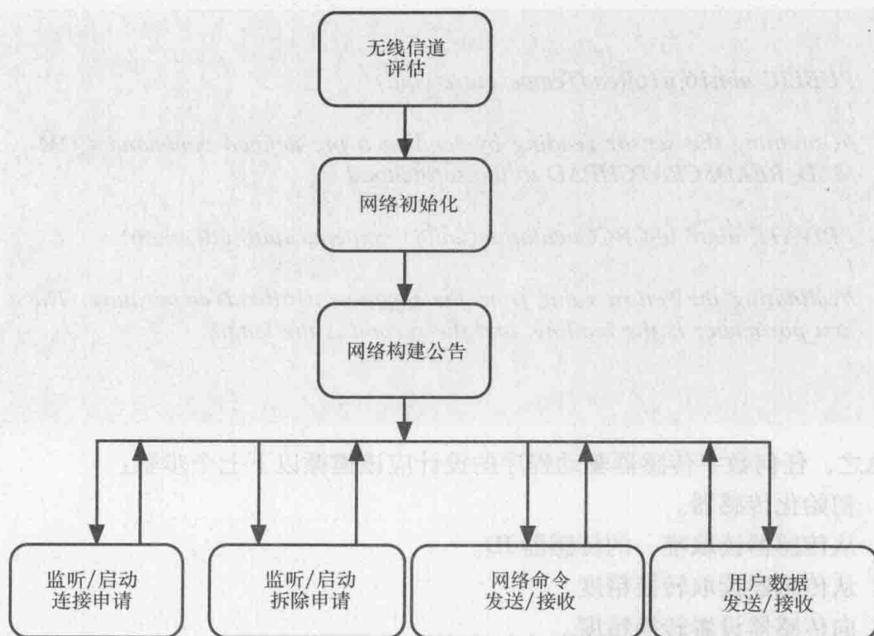


图 4.13 构建 WSN 的过程

```
void vAppApiMlmeRequest(
    MAC_MlmeReqRsp_s *psMlmeReqRsp,
    MAC_MlmeSyncCfm_s *psMlmeSyncCfm);
```

vAppApiMlmeRequest 例程将网络层或应用的 MLME 请求传递到 MAC 层。psMlmeReqRsp 参数是一个包含 MLME 请求的结构体指针。psMlmeSyncCfm 参数是一个包含 MLME 请求结果的结构体指针。

```
void vAppApiMcpsRequest(
    MAC_McpsReqRsp_s *psMcpsReqRsp,
    MAC_McpsSyncCfm_s *psMcpsSyncCfm);
```

vAppApiMcpsRequest 例程将网络层或应用的 MCPS 请求传递到 MAC 层。psMcpsReqRsp 参数是一个包含 MCPS 请求的结构体指针。psMcpsSyncCfm 参数是一个包含 MCPS 请求结果的结构体指针。

构建基于 IEEE 802.15.4 的 WSN 需要许多其他的函数。图 4.14 给出了构造网络层和 MAC 层之间接口的函数（调用与回调）概述。这些调用函数允许网络层向 MAC 层发出请求，然后回调函数允许 MAC 层向网络层请求分配缓冲空间并将信息传回网络层。

- 无线信道评估

当 IEEE 802.15.4 网络 PAN 协调器启动 WSN 时，无线信道评估是第一个将被

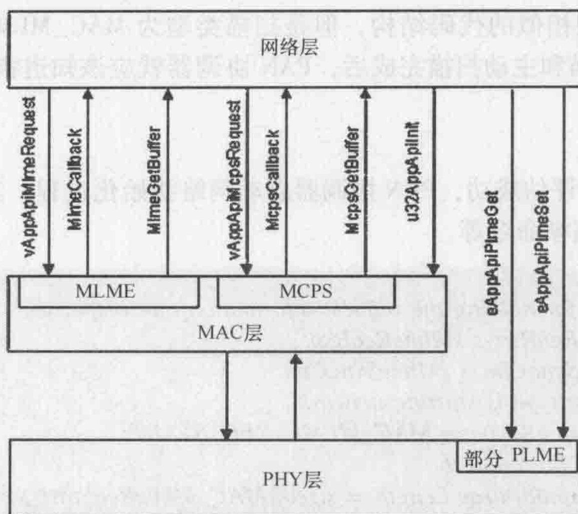


图 4.14　网络层、MAC 层和 PHY 层之间接口概述

执行的任务。PAN 协调器应当确保所需信道是可用的并且不存在网络冲突。

下面的代码段通过调用 vAppApiMlmeRequest(　) 来提交能量扫描请求。在这个函数中需要两个参数。第一个参数是一个指向数据结构 MAC_MlmeReqRsp_s 的指针。该结构包含了对 MLME 的请求，如扫描类型、扫描持续时间和扫描信道等。第二个参数是一个指向数据结构 MAC_Mlme-SyncCfm_s 的指针，该结构包含了 MLME 请求的结果。

```
#define SCAN_CHANNELS 0x07FFF800UL
#define ENERGY_SCAN_DURATION 3
//Structures to hold the parameters for scan request and scan response
MAC_MlmeReqRsp_s sMlmeReqRsp;
MAC_MlmeSyncCfm_s sMlmeSyncCfm;
//The request type is scan
sMlmeReqRsp.u8Type = MAC_MLME_REQ_SCAN;
//The size of the request
sMlmeReqRsp.u8ParamLength = sizeof(MAC_MlmeReqStart_s);
//The scan type is energy scan
sMlmeReqRsp.uParam.sReqScan.u8ScanType = MAC_MLME_SCAN_
TYPE_ENERGY_DETECT;
//Set scan channels
sMlmeReqRsp.uParam.sReqScan.u32ScanChannels = SCAN_CHANNELS;
//Set the scan duration
sMlmeReqRsp.uParam.sReqScan.u8ScanDuration = ENERGY_SCAN_z
zDURATION;
//Submit energy scan request
vAppApiMlmeRequest(&sMlmeReqRsp, &sMlmeSyncCfm);
```

主动扫描使用相似的代码结构，但是扫描类型为 MAC_MLME_SCAN_TYPE_ACTIVE。能量扫描和主动扫描完成后，PAN 协调器就应该知道指定信道和网络标识符是否可用。

● 网络初始化

如果无线信道评估成功，PAN 协调器启动网络初始化过程，其中包括信道数、网络 ID、信标和超帧命令等。

```
//Structures for holding the request information and response
MAC_MlmeReqRsp_s sMlmeReqRsp;
MAC_MlmeSyncCfm_s sMlmeSyncCfm;
//The request type is starting network
sMlmeReqRsp.u8Type = MAC_MLME_REQ_START;
//The size of the request
sMlmeReqRsp.u8ParamLength = sizeof(MAC_MlmeReqStart_s);
//The network ID. Make sure it does not conflict with other PANs in the vicinity
sMlmeReqRsp.uParam.sReqStart.u16PanId = 0x1234;
//Define the working channel
sMlmeReqRsp.uParam.sReqStart.u8Channel = CHANNEL_CLEAN;
//Define the beacon order and superframe order. The duty cycle is 50 % in this case
sMlmeReqRsp.uParam.sReqStart.u8BeaconOrder = 0x03;
sMlmeReqRsp.uParam.sReqStart.u8SuperframeOrder = 0x02;
//The network is started by the PAN coordinator
sMlmeReqRsp.uParam.sReqStart.u8PanCoordinator = TRUE;
```

● 网络构建公告

网络构建公告的过程是由使用的网络协议决定的。网络构建公告实际上是通过定期发送信标信号来完成的。如果协议不支持定期信标信号的发送，那么它应该能够对那些执行无线信道评估的设备发出的任何有效的请求进行响应。

```
//Regularly sending the beacon signals
vAppApiMlmeRequest(&sMlmeReqRsp, &sMlmeSyncCfm);
```

● 监听/启动连接申请和监听/启动拆除申请

和其他无线网络一样，WSN 应能够扩展它的覆盖范围或者通过采用新设备扩大容量，或者在收到有效指令时能移除现存的网络设备。WSN 的网络协议栈必须支持预定义机制来处理这种网络变化。

为了避免创建重复的设备记录，IEEE 802.15.4 协议栈提供了一个简单的机制。通过检查设备请求的唯一 64 位扩展地址，PAN 协调器能够确定这个设备是否已经在本地列表里存在。如果存在，将授权相同的 16 位网络地址给这个请求。如

果不存在于本地列表里，并且有可用空间供任何采用的新设备使用，通过先前分配的 16 位网络地址加 1 的方式来授权一个新的 16 位网络地址给这个请求。在下面的代码段中，16 位网络地址存于变量 u16ShortAdr 中。连接申请和拆除申请分别通过提交的请求类型 MAC_MLME_RSP_ASSOCIATE 和响应 MAC_MLME_RSP_DISASSOCIATE 来实现。MAX_END_DEVICES 是 PAN 协调器能够接入的设备的最大值。终端设备的当前数量存于 numEndDevices 中。

```
MAC_MlmeReqRsp_s sMlmeReqRsp;
MAC_MlmeSyncCfm_s sMlmeSyncCfm;
//The address of end devices starts from 0x0000
#define END_DEVICE_START_ADR 0x0000
uint16 u16ShortAdr = 0;
//If local space is still available
if (PANCoordinator.numEndDevices < MAX_END_DEVICES)
//Generate a new 16-bit network address
u16ShortAdr = END_DEVICE_START_ADR
+ PANCoordinator. numEndDevices;
//Create the association response. The request type is associate response
sMlmeReqRsp.u8Type = MAC_MLME_RSP_ASSOCIATE;
//Length of response
sMlmeReqRsp.u8ParamLength = sizeof(MAC_MlmeRspAssociate_s);
//Store the 16-bit address of the new device
sMlmeReqRsp.uParam.sRspAssociate.u16AssocShortAddr = u16ShortAdr;
//Submit the associate response
vAppApiMlmeRequest(&sMlmeReqRsp, &sMlmeSyncCfm);
```

与连接申请不同，拆除申请由网络设备发起。请求类型是 MAC_MLME_RSP_ASSOCIATE，16 位网络地址是协调器的短地址，可表示为 CoordShortAddr。

```
/Structures for holding the disassociate request
MAC_MlmeReqRsp_s sMlmeReqRsp;
MAC_MlmeSyncCfm_s sMlmeSyncCfm;
//The request type is disassociate request
sMlmeReqRsp.u8Type = MAC_MLME_REQ_DISASSOCIATE;
//Length of response
sMlmeReqRsp.u8ParamLength = sizeof(MAC_MlmeReqDisassociate_s);
//the 16-bit address disassociated with
sMlmeReqRsp.uParam.sReqDisassociate.sAddr.uAddr.u16Short
= CoordShortAddr;
//Submit the disassociate request
vAppApiMlmeRequest(&sMlmeReqRsp, &sMlmeSyncCfm);
```

● 网络命令发送与接收

网络命令对于用户来说通常是不可见的，但是有时也需要用户的干预。一个健壮的网络应该通过实现必要的算法来处理网络内部发生的各种事件而不需用户的干预。但是，应用软件仍然需要在网络管理方面保持可管理的能力。例如，当网络系统为采用的新设备增强安全等级时，任何请求设备的细节信息需要由上层管理系统审核，而不是由协议栈本身自动决定。网络命令的发送与接收也可以通过提交相应的请求来执行。

```
//Submitting the request when required
vAppApiMlmeRequest(&sMlmeReqRsp, &sMlmeSyncCfm);
```

● 用户数据发送与接收

如本书 2.3.7 节所述，在信标使能网络中，用户数据的发送与接收只能间接使用时隙 CSMA/CA；但是在非信标使能网络中，可以直接或者间接使用非时隙 CSMA/CA。下面的代码显示了从协调器到网络设备的间接传输。当协调器向网络设备发送一个数据包时，协调器将数据存储在本地缓冲区（在下面例子的域 sFrame. au8Sdu）中，并且将地址等待列表（这里是 pu8Payload）与数据包信息进行关联。最后通过调用网络层或者应用到 MCPS 的函数 vAppApiMcpsRequest 来提交数据发送/接收请求。

```
//Structures for holding the data transmission request
MAC_McpsReqRsp_s sMcpsReqRsp;
MAC_McpsSyncCfm_s sMcpsSyncCfm;
//a pointer to the outgoing packet
uint8 *pu8Payload;
//The request type is data request
sMcpsReqRsp.u8Type = MAC_MCPS_REQ_DATA;
sMcpsReqRsp.u8ParamLength = sizeof(MAC_McpsReqData_s);
//Generate an id for the outgoing data packet
sMcpsReqRsp.uParam.sReqData.u8Handle = u8CurrentTxHandle;
//Prepare the coordinator ID (PAN-ID) and 16-bit short address
COORDINATOR_ADR as//the source address
sMcpsReqRsp.uParam.sReqData.sFrame.sSrcAddr.u16PanId = PAN_ID;
sMcpsReqRsp.uParam.sReqData.sFrame.sSrcAddr.uAddr.u16Short =
COORDINATOR_ADR;
//Prepare the destination 16-bit short address for transmission
sMcpsReqRsp.uParam.sReqData.sFrame.sDstAddr.u16PanId = PAN_ID;
sMcpsReqRsp.uParam.sReqData.sFrame.sDstAddr.uAddr.u16Short =
u16DestAdr;
//Use indirect transmission for a coordinator to generate data request. The
data will be stored in the local buffer until being fetched by the network
```

```
device, rather than directly//transmitting to the network device. Acknowl-
edgement is required.
sMcpsReqRsp.uParam.sReqData.sFrame.u8
TxOptions = (MAC_TX_OPTION_ACK|MAC_TX_OPTION_INDIRECT);
//Link the address of the pu8Payload to the corresponding component in the
outgoing//packet.
pu8Payload = sMcpsReqRsp.uParam.sReqData.sFrame.au8Sdu;
//Put the data into the packet
.......
//Finally, store the payload length in the structure
sMcpsReqRsp.uParam.sReqData.sFrame.u8SduLength = EFFECTIVE_
PAYLOAD;
//Submit the data transmission request
vAppApiMcpsRequest(&sMcpsReqRsp, &sMcpsSyncCfm);
```

4.5 无线传感器网络与外部公共网络的桥接

WSN 旨在用来收集传感器数据并将收集到的数据通过网关传输到本地或远程数据处理站。其中的网关可以是 ZigBee 网络的汇聚节点或 6LowPAN 网络的边界路由器。本地或远程数据处理站通常运行在具有不同通信协议的公共网络中。通常，WSN 与 Wi-Fi 系统互联，然后 WSN 通过 Wi-Fi 系统与因特网互联。图 4.15 给出了 4 节点 WSN 与公共网络互联示例。

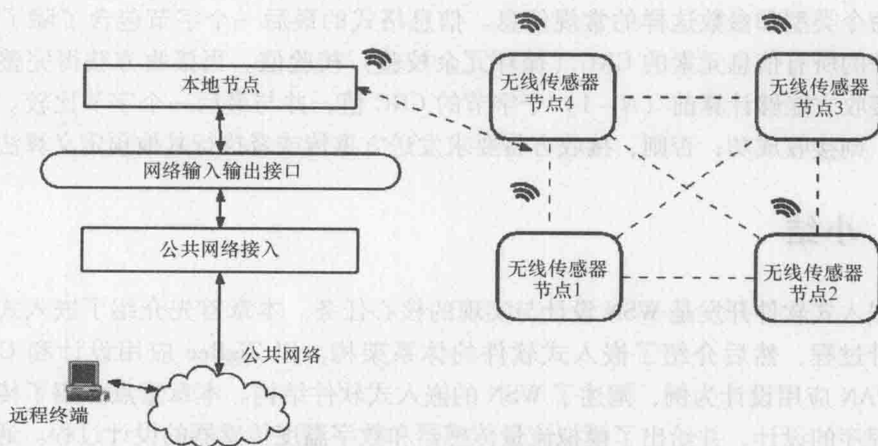


图 4.15 4 节点 WSN 与公共网络互联示例

表 4.2 网络输入输出接口的信息格式

字节 1	命令长度（1 ~ N）
字节 2	命令类型
字节 3	参数 1
字节 4	参数 2
⋮	⋮
字节 N	CRC（循环冗余校验）

在图 4.15 中，本地节点是一个汇聚节点或者边界路由器。所有收集到的信息从单个传感器节点送到本地节点。然后信息传输到公共网络接入，公共网络接入有一个特殊设计的协议用来处理从公共网网络到远程终端的数据传输。从远程终端到 WSN 传送的指令应沿着相反的路径传输。由于公共网络和 WSN 通常使用不同的协议，因此网络输入和输出接口需要执行两个系统间的翻译功能。在大多数情况下，网络输入和输出接口需要设计特殊的硬件来完成。例如，在智能家居（Gil 等，2009）中，Wi-Fi 和基于 ZigBee 的 WSN 之间的连接是通过将 Digi connect Me 模块（Digi International，2010）与英国 Jennic 公司的 ZigBee 芯片 JN5139 的高速串行接口（如 UART）进行连接来实现的（Gill 等，2009）。

对于嵌入式软件设计者来说，在数据发送和接收期间，实现某种错误检查机制来检错是非常重要的。表 4.2 给出的网络输入和输出接口的信息格式是一种简单的双方接口信息格式。

表 4.2 中，信息格式由一系列字节组成。第一个字节包含了整个信息的长度。在接收到第一个字节时，接收方就能够确定当前传输需要多少字节。信息主体包含了像命令类型和参数这样的常规信息。信息格式的最后一个字节包含了除了 CRC 字段外的所有信息元素的 CRC（循环冗余校验）校验值。当接收方获得完整信息后，接收方能够计算前（$N-1$）个字节的 CRC 值，并与最后一个字节比较。如果匹配，则接收成功；否则，接收方将要求发送方重传或者执行其他预定义算法。

4.6 小结

嵌入式软件开发是 WSN 设计与实现的核心任务。本章首先介绍了嵌入式软件的设计过程，然后介绍了嵌入式软件的体系架构。以 ZigBee 应用设计和 Contiki 6LowPAN 应用设计为例，阐述了 WSN 的嵌入式软件结构。本章重点介绍了传感器驱动程序的设计，并给出了模拟流量传感器和数字温度传感器的设计过程。通过使用 IEEE 802.15.4 协议栈的代码段阐述了实现 WSN 的过程。本章主要是针对 WSN 的设计过程和基本的嵌入式软件编码来进行探讨的。由于编码因系统而异，所以忽略了编码的语法细节。

参考文献

Contiki Wiki: Processes. http://www.sics.se/contiki/wiki/index.php/Processes#Autostarting_Processes (2012)

Digi International: http://www.digi.com/pdf/prd_ds_digiconnectfamily_usersguide.pdf (2010)

Gems Sensor: FT110 Flow sensor. http://docs-europe.electrocomponents.com/webdocs/023e/0900766b8023e8ed.pdf (2008)

Gill, K., Yang, S.H., Yao, F., Lu, X.: A Zigbee-based home automation system. IEEE Trans. Consum. Electron. **55**(2), 422–430 (2009)

Jennic: Jennic 802.15.4 Stack API Reference Manual. http://www.jennic.com/files/support_files/JN-RM-2002-802.15.4-Stack-API-1v8.pdf (2008a)

Jennic: ZigBeeStackUserGuide. http://www.jennic.com/files/support_files/JN-UG-3017-ZigBeeStackUserGuide-1v6.pdf (2008b)

Jennic: IEEE 802.15.4 Application Development Reference Manual. http://www.jennic.com/files/support_files/JN-RM-2024-IEEE802.15.4-App-Dev-2v0.pdf (2010)

Labrosse, J., Ganssle, J., Noergaard, T., Oshana, R., Walls, C., Curtis, K., Andrews, J., Katz, D.J., Bentile, R., Hyder, K., Perrin, B.: Embedded Software. Elsevier, Amsterdam (2008)

Laplante, P.A.: Real-Time Systems Design and Analysis. Wiley, New York (2004)

Maxim: DS18B20 Programmable Resolution 1-Wire Digital Thermometer. http://pdfserv.maxim-ic.com/en/ds/DS18B20.pdf (2009)



第 5 章　无线传感器网络中的路由技术

关键词：路由协议　AODV 簇树　能量感知路由

5.1　引言

路由协议是一种位于网络层的软件，负责决定一个输入的数据包应被哪个输出路由传送出去。换句话说，它是一种算法，用于寻找从源节点到目的节点数据传输的路由。目的节点通常被称为汇聚节点或 WSN 中的基站。这可能是一段距离源节点很远的距离，甚至超出该节点的传输范围。因此，数据在到达汇聚节点之前可能不得不进行多跳。图 5.1 给出了一个从传感器到一个汇聚节点的通信路由。然而，由于 WSN 的特性和各种约束，已有的为有线网络和其他如移动自组网（Mobile Ad-hoc Network，MANET）的无线网络设计的路由协议不适合 WSN。WSN 路由的典型特征和约束条件如下所述（Al-Karaki 和 Kamal，2004）：

- WSN 路由协议的一个主要目标是保存能量和降低消耗，而其他网络路由协议却被设计成在数据传输过程中去实现高 QoS。
- 无线传感器节点有许多限制，如有限的能量供应、有限的内存大小、有限的计算能力、无线传感器之间无线信道的有限带宽等。
- 一个 WSN 可能含有大量的传感器节点，因此使用一个全局标识地址来访问每个单独的节点可能是不可行的。
- 一个 WSN 可能有不同的应用需求，因此 WSN 的设计应该是面向特定应用的。
- 路由协议应消除检测到的数据冗余，这些冗余产生于许多无线传感器节点在同一时间感知同一环境现象的时候。为了减少冗余，数据融合是必需的，包括重复数据压缩、数据融合等。
- 由于传感器较低的成本和电池驱动，在 WSN 中的传感器节点很容易出现错误或故障。因此，即使网络中有节点出现故障，路由协议也应正常有效地发挥作用。这种

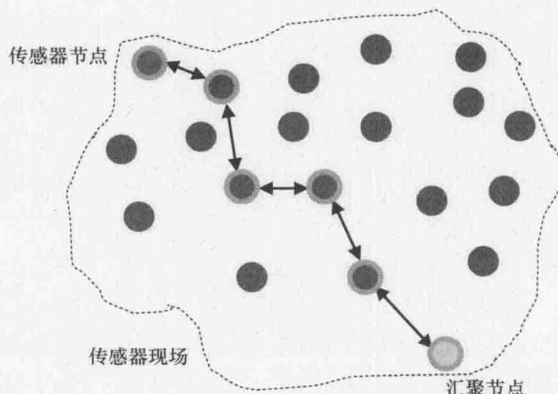


图 5.1　从一个传感器到一个汇聚节点的通信路由

容错功能要求路由协议应该具有通过发现和维护一个新的路由来传输数据，从而具有克服网络中任何故障的能力。

5.2　无线传感器网络中的路由协议分类

路由协议通常可以依据路由确定的方式分为主动式或反应式。主动式路由协议依据通信要求事前确定所有路由，以及在网络拓扑结构发生变化时更新路由。当一个数据发送请求产生时，通信路由可以不经任何进一步的计算从可用的路由表找出并被采用，因此不产生用于数据传输的额外延迟。但是主动路由协议并不适用于网络拓扑结构不断变化的 Ad-hoc 网络。另一方面，反应式路由协议只调用按需路由发现过程。该反应式路由协议适用于动态网络。但确定路由的时间是非常重要的，有可能导致数据传输中延迟的增加。

还有很多根据不同标准进行路由协议分类的其他的方法。图5.2给出了另一种路由协议的分类，所有的路由协议被分类为基于网络结构或者基于协议操作的路由协议。基于网络结构的路由协议有三个子类：平面、分层和基于物理位置的路由协议。基于协议操作的路由协议有五个子类：基于查询的、基于协商的、基于多路由的、基于 QoS 的和基于相干的路由（Vidhyapriya 和 Vanathi，2007；Akkaya 和 Younis，2005）。这些类别和子类别不是相互排斥的，因为某些路由协议可以依据一个以上的类别和子类别进行分类。本节只简要回顾基于网络结构的路由协议。

网络结构可以划分为平面的、分层的或基于位置的。在平面网络中，所有传感器节点位于同一个平面内，具有相同的功能和职责。它们将数据转发送到自己的邻居节点不需要任何相关的网络拓扑结构支持。另一方面，分层网络的传感器节点需要扮演不同的角色，并且它们在逻辑上位于不同的层次。很多的分层网络被划分成不同的簇，每个簇指定一个簇头汇聚和中继簇间数据的传输。基于位置的路由协议依赖传感器节点的物理位置（Vidhyapriya 和 Vanathi，2007；Jolly 和 Latifi，2006）。

5.2.1　平面路由协议

平面路由协议使用以数据为中心的路由协议传送数据，它有一个响应发送请求和查询其他节点并等待它们答复的基站。数据消除和协商可以用来节省网络中的能源。一个在网络拓扑结构中的路由发现过程可以在不注意任何更新的情况下通过泛洪或数据广播到所有邻居节点来启动。本节将讨论最热门的平面路由协议。

5.2.1.1　泛洪路由协议

泛洪路由协议是最基本的平面路由协议，可以很容易地在 WSN 中实现，因为它不需要任何复杂的算法编程。泛洪协议只是将数据广播到所有邻居节点，而不考虑拓扑结构或网络结构（Jolly 和 Latifi，2006）。然后，数据可以通过重复相同的广播过程传输到目的节点，如图5.3所示。虽然，这个协议很简单并且易于实现，但

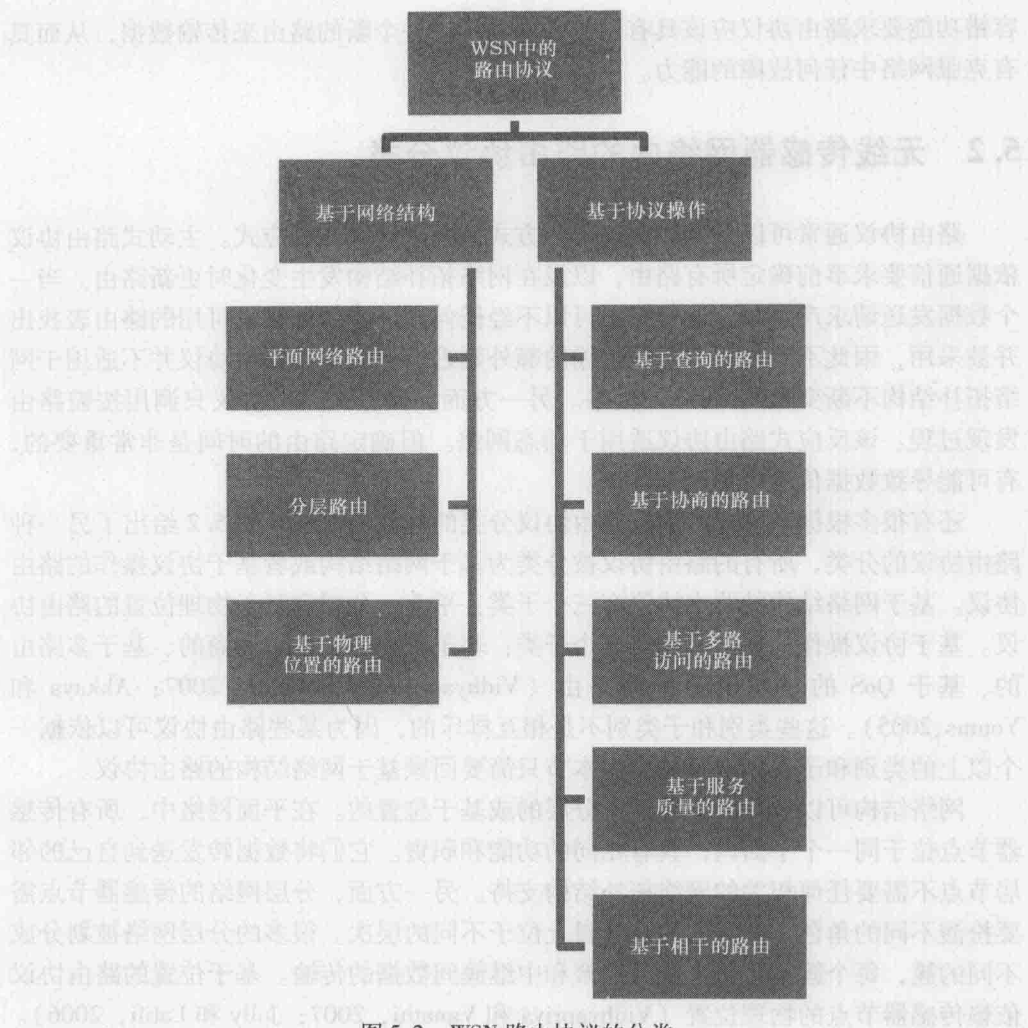


图 5.2 WSN 路由协议的分类

是它存在一些问题。其中一个问题是，许多节点产生大量重复信息。另一个问题被称为内爆，因为每个节点将接收到的数据发送给它的邻居节点，却不知道邻居节点之前是否已经接收到这些数据，当某个节点接收到两次相同的数据时就会发生内爆。图 5.3 所示的节点 G 显示了内爆问题。

5.2.1.2 通过协商的传感器信息协议

通过协商的传感器信息协议（Senser Protocol for Information via Negotiation，SPIN）是另一种平面的路由协议，SPIN 是泛洪协议的更新版本。SPIN 为协议增加了一个协商系统，代替一开始就将数据发送到所有邻居节点，SPIN 首先请求对传输数据感兴趣的节点，然后才发送数据给那些已经表示有兴趣的节点。数据包有三种类型：广告（Advertisement，ADV）、请求（Request，REQ）和数据（DATA）。

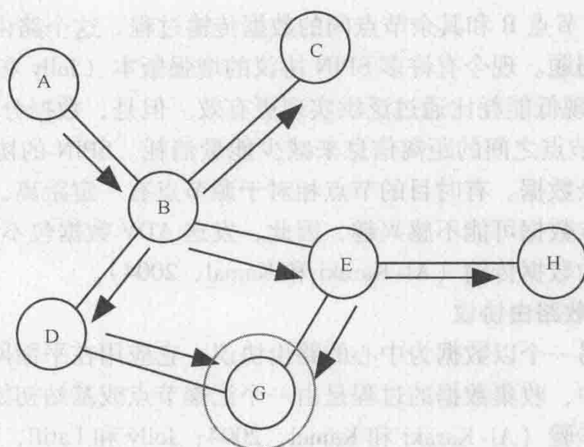


图 5.3 带有内爆问题的泛洪协议

一个有数据的传感器节点向全体邻居节点发送 ADV 数据包。这个 ADV 数据包包括有关传感器的数据信息。如果接收到该 ADV 数据包的节点中的一个之前已经接收过了这些数据，它会忽略 ADV 数据包。否则，它会发送 REQ 数据包回源节点。最后，源节点将通过发送一个包含传感器数据的 DATA 数据包将数据仅传送给这些回应的节点。这个过程反复进行，直到目的节点接收到源传感器数据。图 5.4 给出了 SPIN 过程，图 5.4a ~ c 给出了发生在节点 A 与节点 B 之间的三个步骤，

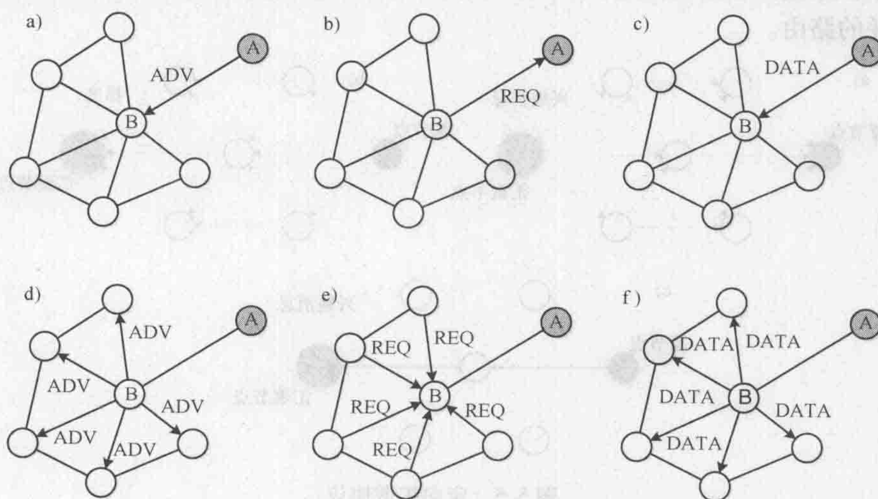


图 5.4 SPIN 过程

a) ADV 数据包从 A 传送到 B b) REQ 数据包从 B 传送到 A

c) DATA 数据包从 A 传送到 B d) ADV 数据包从 B 传送到其余节点

e) REQ 数据包从其余节点传送到 B f) DATA 数据包从 B 传送到其余节点

图 5.4d ~ f 给出了节点 B 和其余节点间的数据传输过程。这个路由协议试图解决重复数据包和内爆问题。现今有许多 SPIN 协议的增强版本（Jolly 和 Latifi，2006）。

利用 SPIN 实现低能耗比通过泛洪实现更有效。但是，数据分配比例是相似的。SPIN 不使用邻居节点之间的距离信息来减少能量消耗。SPIN 的协商系统减少了所产生的一半的冗余数据。有时目的节点相对于源节点有一定距离，而更靠近源节点的节点却对源节点数据可能不感兴趣，因此，发送 ADV 数据包不能保证对 WSN 中远端感兴趣节点的数据传输（Al-Karaki 和 Kamal，2004）。

5.2.1.3　定向扩散路由协议

定向扩散是另一个以数据为中心的路由协议，它应用在平面网络架构中。在定向扩散路由协议中，收集数据的过程是由一个汇聚节点或基站初始化的。这个过程发生在如下三个步骤（Al-Karaki 和 Kamal，2004；Jolly 和 Latifi，2006）：

- 步骤 1。汇聚节点广播一个兴趣数据包到所有邻居节点，而这些邻居节点又将转发兴趣数据包到它们所有的邻居节点，直到兴趣消息到达具有此种兴趣类型数据的源节点。兴趣消息包括一个梯度值，其中包含属性值和梯度方向。步骤 1 如图 5.5a 所示。
- 步骤 2。拥有请求数据的源节点将数据包发送到由梯度决定的存在多条路由的汇聚节点。步骤 2 如图 5.5b 所示。
- 步骤 3。最佳路由由汇聚节点实施加强，如图 5.5c 所示。在梯度值基础上选择最佳路由依赖应用而定，例如，某些应用需要最短路由，其他应用需要最低能源消耗的路由。

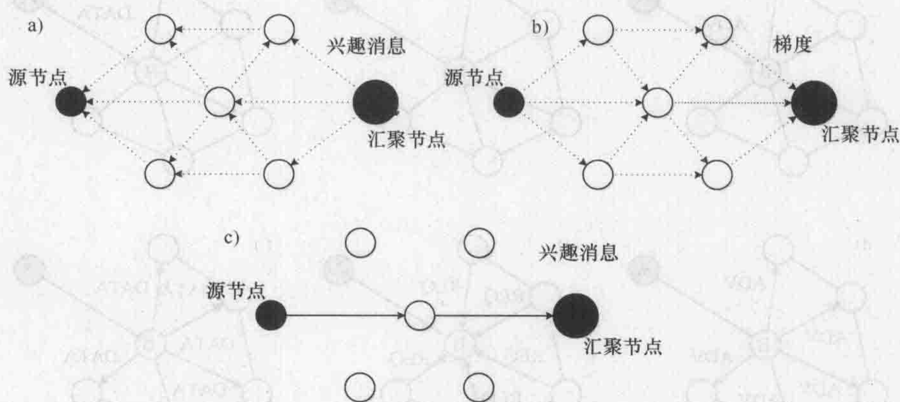


图 5.5　定向扩散协议

a）兴趣消息从汇聚节点传送到源节点　b）数据从源节点传送到汇聚节点

c）从源节点到汇聚节点的最佳路由

定向扩散与 SPIN 或泛洪路由协议不同。定向扩散的数据请求数据包总是从汇聚节点传送到无线传感器节点，而在 SPIN 中是由无线传感器节点做广播，它们有

数据要发送，并允许任何有兴趣的节点来请求它。在另一方面，定向扩散中所有的传输是邻居节点到邻居节点的沟通，所有的节点都拥有数据汇聚和高速缓存的能力。定向扩散路由协议并不要求确定的网络拓扑结构，可能不适合需要连续数据传输的应用。

5.2.2　分层路由协议

分层路由最初是一种有线网络路由协议。然而，它也适用于增强可扩展性和通信效率的无线网络。分层路由协议的主要概念依赖将无线传感器节点分解到一个以上的层次。大多数分层路由协议包括两个路由层次：第一个层次负责选择簇头；第二个层次是有关路由的决策。例如，需要实现非常低的能耗的分层路由协议，可以根据传感器节点的能量水平划分传感器节点。处于高能量水平的节点可以被分配来处理和传送数据，同时具有较低能量水平的节点则只是被分配来感知事件。网络节点内簇的形成可以提高传感器节点的效率和可扩展性。有许多的分层路由协议，本节仅给出一些最常用的协议。

5.2.2.1　低能量自适应分层协议

低能量自适应分层（Low Energy Adaptive Clustering Hierarchy，LEACH）协议主要用来解决节约能源和减少通信能量消耗的问题。在 LEACH 协议中，一些无线传感器节点被随机选择充当簇头。通过重复这个簇头的选择过程，无线传感器节点将分享能源消耗。如果簇头是固定的，那么它们将因为比普通节点消耗更多的能量而很快消亡，这将防止其他相连的节点加入到网络中。LEACH 协议工作在两个独立的阶段：第一阶段是簇建立阶段，包括定义簇头；第二阶段是稳定运行阶段，包括传输数据。在簇建立阶段，一组节点（P）选择自己充当簇头。这些节点在0和1之间选择一个随机数。如果该随机数大于一个阈值 $T(n)$，则节点 n 不能作为一个簇头节点。阈值 $T(n)$ 计算如下：

$$T(n)=\begin{cases}\dfrac{p}{1-p\times[r\bmod(1/p)]} & \text{当 } n\in G\\[2ex] 0 & \text{其他}\end{cases}\tag{5.1}$$

式中，p 为节点成为簇头节点的预期百分数；

r 为当前轮数；

G 为在最近的一轮中 $1/p$ 未当选簇头的节点集合。

所有指定的簇头发送 ADV 数据包给所有非簇头节点来确定它们归属的簇，如图5.6所示。收到这则 ADV 后，非簇头节点将确定它们想要加入的簇头。这一决定主要依据接收到的来自簇头发送过来的信息的信号强度。因此，非簇头节点会选择需要通信能量最低的簇头节点。在此之后，非簇头节点将向其他簇头节点报告它们对簇头节点的选择（Al-Karaki 和 Kamal，2004）。

每个簇头将建立一个对于其簇中的所有节点的 TDMA 时间表。簇中的每个节

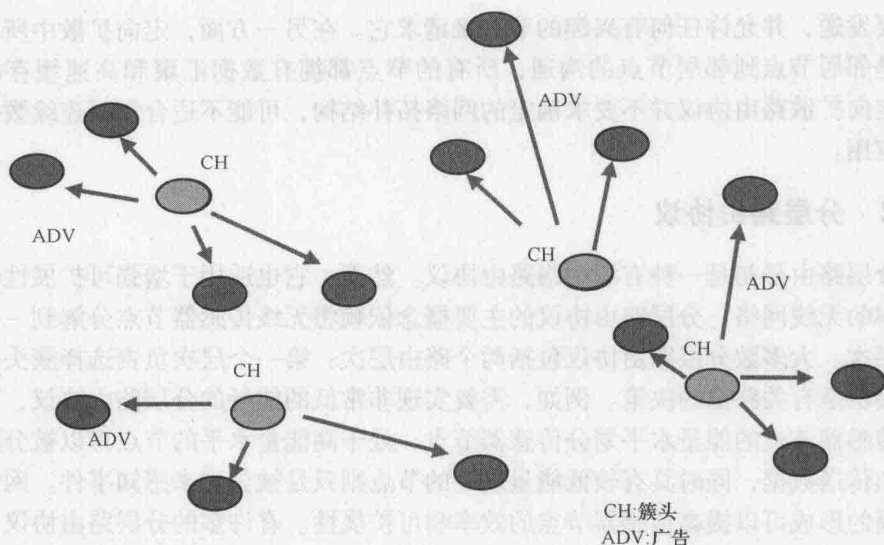


图 5.6 LEACH 协议中邻居节点加入簇头

点将根据时间表调度数据传输到簇头，簇头然后融合数据以减少数据量。最后，融合的数据传送至汇聚节点。LEACH 协议是没有办法系统地分配簇头角色到网络内的传感器节点的。此外，LEACH 协议假定网络中所有的能量水平是相同的，还假定每个节点有数据要在一个特定的时间发送。

5.2.2.2 阈值敏感节能传感器网络

阈值敏感节能传感器网络（Threshold sensitive Energy Efficient sensor Network，TEEN）协议是另一种分层路由协议。不同于 LEACH 协议，它只有一层的分层结构，其网络体系结构是基于多簇分层结构的。图 5.7 给出了一个两层的簇结构，传感器节点与第一层簇头通信，而这些第一层簇头与它们的第二层簇头进行通信。第二层的簇头直接与汇聚节点进行通信。这个过程发生在各个分层，每个簇中的簇头从其簇中的成员收集数据，进行数据融合，并将其发送到上层簇头或汇聚节点。这个多层体系结构增大了传感器网络的覆盖范围；由于一个传感器节点不需要直接与汇聚节点通信，从而减少了电源制约和传感器节点传输范围的影响。低层次簇中的数据在到达汇聚节点之前可以通过多个层次簇头传输。

TEEN 协议（Manjeshware 和 Agrawal，2001）主要用于测量例如温度和压力之类物理现象的应用。TEEN 协议也适合于如火险报警的实时应用。TEEN 协议的传感过程是瞬间发生的，数据是定期发送的。TEEN 协议使用簇来形成发送的数据，簇头传送两个阈值信息给其簇内的非簇头节点：一个是硬阈值，它是属性阀值，超过这个阈值时传感器节点必须打开其传送器并把检测值报告给它的簇头；另一个称为软阈值，它是传感属性数据值变化的限定量，检测值变动大于等于软阈值时同样

触发传送器启动并传送检测值到它的簇头。

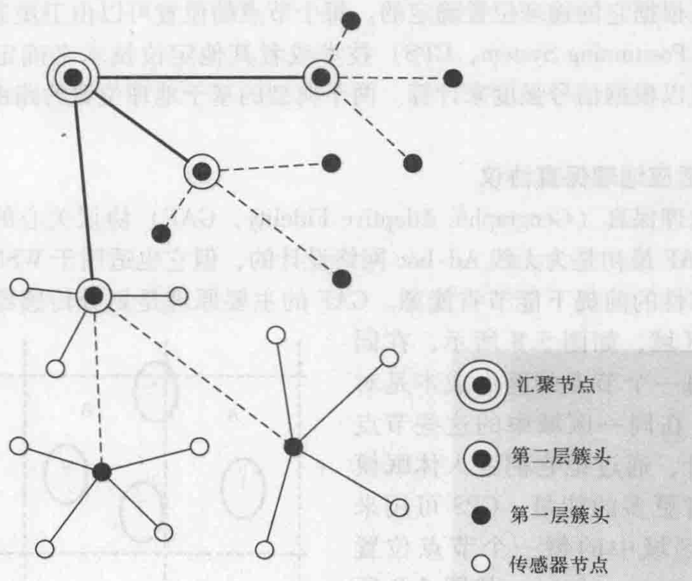


图 5.7　TEEN 分层结构的一个例子

一个 TEEN 协议的增强版本称为自适应阈值敏感节能传感器网络（Adaptive TEEN，APTEEN）协议（Manjeshware 和 Agrawal，2002）。APTEEN 协议的目标是既可以实现主动周期性采集数据，又可以对突发事件作出快速反应。簇头安排时间表向它们簇内的所有无线传感器节点广播硬、软阈值。当这些节点检测到的数据大于硬阈值时，允许传输检测值。无线传感器节点的属性值变化等于或大于软阈值时也将传送数据。一个节点两次连续传送报告给每个节点的最大时间周期称为计数时间，该计数时间为每个节点指定一个特定时间用于发送检测值。如果传感器节点在计数时间内没有传送任何数据，一个 TDMA 调度将为每个这种节点分配一个时间片，并强迫这个节点去检测和传输数据。APTEEN 协议支持以下三种不同的查询类型（Hu 和 Cao，2010）：

- 历史性查询，分析过去的数据。
- 按需查询，快速浏览网络。
- 连续查询，在一段时间内持续监控某一事件。

从提高网络生命周期和节能方面来看，TEEN 协议和 APTEEN 协议的性能优于 LEACH 协议。从另一方面来看，两种协议中形成一个簇的额外开销仍然存在。阈值函数和计数时间的确定增加了应用实现的复杂性和网络内部的开销。

5.2.3　基于地理位置的路由协议

WSN 基于网络结构的第三类路由协议是基于地理位置的路由协议。这一类路

由协议的主要思想是在数据路由过程中利用无线传感器节点的地理位置优势。每个节点的地址是根据它的物理位置确定的。每个节点的位置可以由卫星通过全球定位系统（Global Positioning System，GPS）技术或者其他定位技术来确定。其到邻居节点的距离可以根据信号强度来计算。两个典型的基于地理位置的路由协议将在本节描述。

5.2.3.1 自适应地理保真协议

自适应地理保真（Geographic Adaptive Fidelity，GAF）协议关心的主要是能量感知问题。GAF 最初是为无线 Ad-hoc 网络设计的，但它也适用于 WSN。GAF 在不影响路由可靠性的前提下能节省能源。GAF 的主要原理是划分传感器区域为固定的虚拟网格区域，如图 5.8 所示，在同一区域中的每一个节点的路由成本是对等的。因此，在同一区域中的这些节点可以忽略不计，通过把它们置入休眠模式，从而节省更多的能量。GPS 可用来确定在相同区域中的每一个节点位置（Xu 和 Heidemann，2001）。如图 5.8 所示，一个传感器区域划分成区域 A、B 和 C。节点 1 位于区域 A 中，节点 2、3 和 4 都位于区域 B，节点 5 是位于区域 C。r 代表虚拟网格的大小。节点 1 和 5 可以与节点 2、3 和 4 进行通信，但是节点 1 和 5 不能直接地相互通信，因为它们相应地属于区域 A 和 C，被区域 B 所分开。

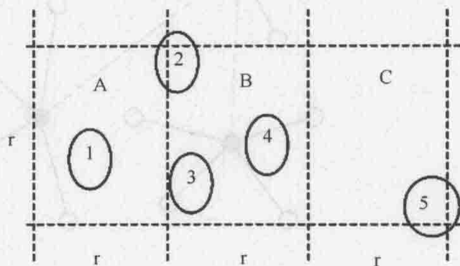


图 5.8 GAF 中的虚拟网格区域

GAF 中有三个阶段：发现阶段、活动阶段和休眠阶段。发现阶段包括发现同一网格内的每个节点的邻居节点；在活动阶段，节点参与路由数据；休眠阶段包括关闭该节点的传送器和设置该节点为休眠模式。在图 5.8 所示的区域 B 的节点 2、3 和 4 中的两个节点可以在同一时间被关闭，只保持其中一个清醒来进行通信。很明显，这个路由协议依赖 GPS 技术来确定无线传感器节点的位置，它并不总是可用的，特别是对于室内应用。此外，为了存储每个节点的邻居地址该路由协议会在存储器单元上产生额外的开销。

5.2.3.2 地理与能量感知路由协议

地理和能量感知路由（Geographic and Energy Aware Routing，GEAR）协议（Yu 等，2001）试图将数据传输到目标区域内的所有节点，这是以数据为中心的 WSN 应用中很常见的。GEAR 协议使用地理信息将数据路由到一个网络中的特定区域。这个过程取决于能量和邻近区域的地理信息。GEAR 协议的主要思想是通过只发送兴趣数据包到网络中的某些区域或方向来减少兴趣数据包的数量，而不是像定向扩散（Direct Diffusion，DD）那样传送兴趣数据包到整个网络。这将比 DD 节省更多的能量。

在GEAR协议中，每个节点保持两个值：估计成本和学习成本。估计成本综合考虑了与目标区域的距离和节点的剩余能量。当某个节点的周围没有任何邻居节点比它自身更接近目标区域，将创建网络“洞”，这种环绕网络中“洞”周围路由所引起的估计成本的变化是学习成本，如果网络中没有“洞”，估计成本将等于学习成本。每当一个数据包到达目标区域，该节点的学习成本就要传播到上一跳。基于能量感知的信息，GEAR协议以一种节能的方式智能地选取下一跳邻居节点路由数据到目标区域。一旦数据到达目标区域，GEAR协议将传播数据到该地区的所有节点。

GEAR协议的两个阶段如图5.9所示。第一阶段是向目标区域传输数据包，第二阶段是在目标区域内传输数据包。在第一阶段，收到数据的无线传感器节点要确保至少有一个邻居节点更靠近目标区域。如果有不止一个这样的邻居节点，那么该传感器节点将选择一个最接近目标区域的节点作为数据传输的下一跳节点。如果在到达目标区域的途中没有任何邻居节点比自己更近，那么该节点被标记为网络中的一个“洞”。在第二阶段中，数据包到达目标区域之后，可以利用受限的泛洪方式和递归的地理传输方式发布该数据。

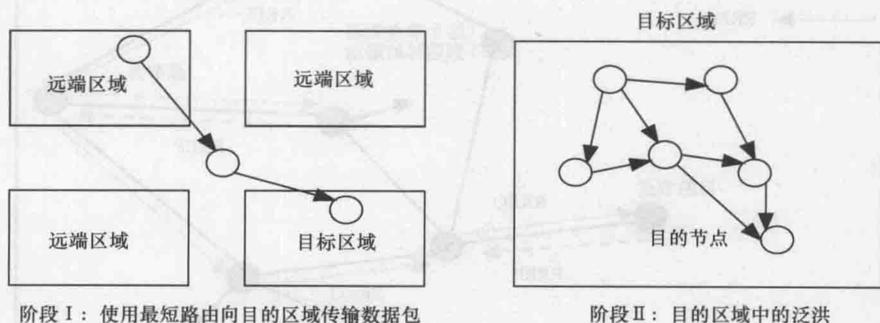


图5.9　GEAR协议的两个阶段

5.3　Ad-hoc网络按需距离矢量路由协议

Ad-hoc网络按需距离矢量（Ad-hoc On Demand Distance Vector，AODV）路由协议是讨论最多的和最先进的路由协议之一。它的主要开发者是Charles E. Perkins（芬兰Nokia公司）和Elizabeth Belding-Royer（美国UCSB）。ZigBee标准在其协议栈中实现了AODV路由协议和摩托罗拉的簇树路由协议，这使得它们被广泛地应用于工业领域。本节介绍AODV路由协议的原理，并给出了AODV路由协议简化版本的实现细节。

5.3.1　Ad-hoc网络按需距离矢量路由协议原理

AODV是一个动态、自启动、多跳的路由协议，它使参与的移动节点建立和维

持一个 Ad-hoc 网络。AODV 路由协议允许移动节点快速获得至新目的的路由，而不需要它在非活动期保留到目的的路由。AODV 路由协议也允许移动节点及时回应断链和网络拓扑结构的变化。

AODV 路由协议中定义了三种类型的消息：路由请求（Route Request，RREQ）、路由应答（Route Replies，RREP）和路由错误（Route Error，RERR）。当需要一个通往新目的的路由时，节点广播一个 RREQ 去寻找通往目的的路由。每个节点在接收到请求后在一个反向表中缓存一个返回发起请求源节点的路由，这样 RREP 可以沿着从目的到发起者的反向路由单播。当 RREQ 到达目的或提供了至目的可达性的节点时，一条路由就可以确定下来了。通过单播 RREP 返回到发起 RREQ 的源节点及在每个节点建立路由表可以确定一条路由，图 5.10 给出了 AODV 路由协议中的 RREQ 和 RREP 传输。

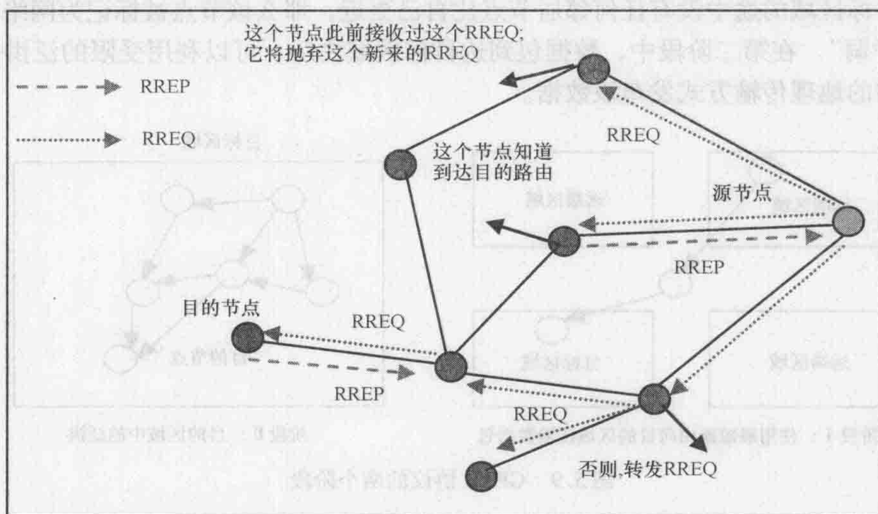


图 5.10　AODV 路由协议中的 RREQ 和 RREP 传输

为了使节点监控活动路由上下一跳的链路状态，一个 HELLO 消息被定期传送出去用以检测在活动路由上的断链，如果没有收到 ACK，则断开的链路是无效的。因此，一个 RERR 消息经常被传输来通知其他节点已发生的断链，该 RERR 消息表明沿着断链路由无法到达目的。

5.3.2　Ad-hoc 网络按需距离矢量路由协议的消息格式

RREQ、RREP 和 RERR 的消息格式已在因特网工程任务组（Internet Engineering Task Force，IETF）的移动 Ad-hoc 网络工作组文件（Perkins 和 Royer，2003）中进行了定义。图 5.11 ~ 图 5.13 给出了这些消息的格式。AODV 路由协议数据报中的字段含义见表 5.1。

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |D|G|           Reserved          |   Hop Count   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            RREQ ID                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination IP Address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Destination Sequence Number                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Originator IP Address                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Originator Sequence Number                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   Next Path Node IP Address                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Next Path Node Sequence Number                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   (additional node IP address and sequence number pairs) ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

图5.11　RREQ消息格式

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |A|Reserved | APN Cnt |Prefix Sz|   Hop Count   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination IP address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Destination Sequence Number                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Originator IP address                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Originator Sequence Number                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   Next Path Node IP Address                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Next Path Node Sequence Number                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   (additional node IP address and sequence number pairs) ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

图5.12　RREP消息格式

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |            Reserved           |   DestCount   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Unreachable Destination IP Address (1)             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Unreachable Destination Sequence Number (1)           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
|  (more node IP address and sequence number pairs as needed) ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

图5.13　RERR消息格式

表 5.1　AODV 路由协议数据包中的字段含义

字　段	描　述
Type	1-RREQ，2-RREP，3-RERR，4-ACK（应答）
D	仅允许目的节点回复标志。如果设置一个中间节点可能不会回应这个 RREQ
G	免费路由回复标志。指示是否向目的节点回复一条免费 RREP
Reserved	填充 0；接收端忽略此字段
Hop count	从发起节点到处理该请求的节点或目的节点的跳数
Dest count	本消息包内包含的不可达目的节点的数目，必须至少为 1
APN count	追加节点到 RREP 中的累计路径的数目
Prefix size	经过相同路径可到达的目的子网内的节点数目
RREQ ID	一个唯一标识特定 RREQ 的序列号
Destination IP address	目的节点的 IP 地址
Destination sequence number	与目标节点相关联的序列号
Originator IP address	发出 RREQ 消息或起始路由（RREP 消息）的发起节点的 IP 地址
Originator sequence number	发起节点的序列号
Next path node IP address	从发起节点到目的节点路径的下一个节点的 IP 地址
Next path node sequence number	从发起节点到目的节点路径的下一个节点的序列号
Unreachable destination IP address	由于断链变得不可达的目的节点的 IP 地址
Unreachable destination sequence number	路由表中之前列出的不可达 IP 地址项对应的目的节点序列号

5.3.3　Ad-hoc 网络按需距离矢量路由协议简化版本的实现

本节给出了在 Contiki 操作系统（Operating System，OS）中 AODV 路由协议简化版本在传感器节点的实现。如图 5.14 所示，一个 WSN 包含四个传感器节点，其中节点 S 需要发送一些检测值到节点 R，节点 S 和 R 不在通信区域内，传送器节点 T_1 和 T_2 是用于中继接收到的消息的两个路由器，节点 R 是目的节点。

最初，当节点 S 不知道至节点 R 的路由时，它必须广播一个 RREQ 消息。节点 T_1 和 T_2 将收到消息，但是因为它们不是目的节点，它们将传送消息给节点 R。这可能会导致冲突，因为这两个节点 T_1 和 T_2 可能是同时传输的。这里已经采用一个非常简单的冲突避免机制：传送器在发送消息之前等待一个随机的时间段。当消息被传输到节点 R，它单播回传一个 RREP 消息给两个传送器

T_1 和 T_2，然后到节点 S。节点 S 可以使用两个标准来确定路由。可以选择较高的 RSSI 路由器或者选择具有最高电池水平的路由器。一旦路由已经被发现，它将被节点 S 用于发送检测值（使用单播消息）到节点 R。路由协议的信息流如图 5. 15 所示。

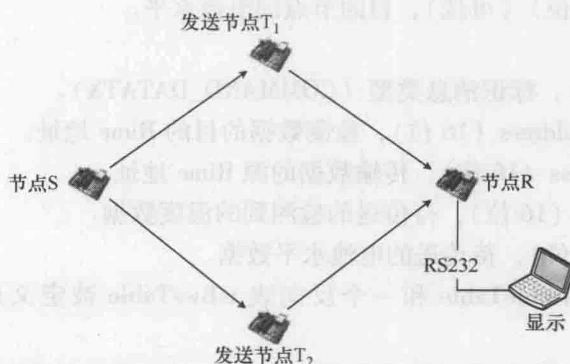


图 5. 14　一个四节点的 WSN

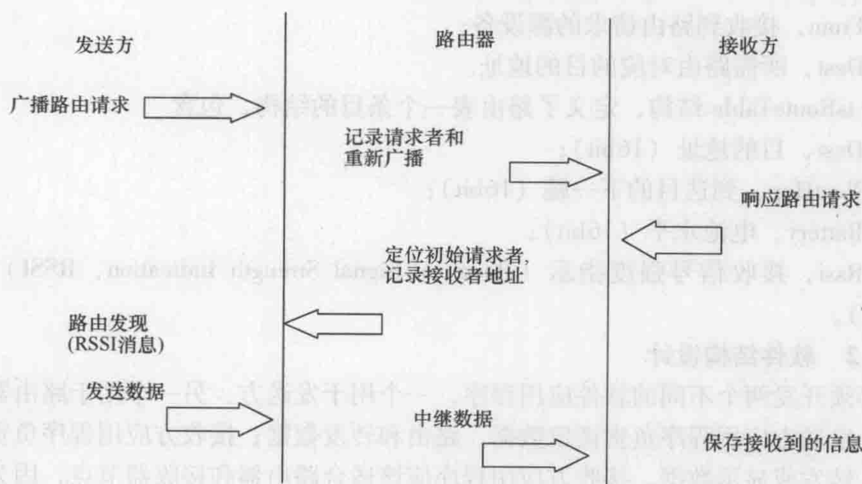


图 5. 15　路由协议的信息流

5. 3. 3. 1　消息类型

三种消息类型定义如下：

路由请求消息

- Type（8 位），标识消息类型（COMMAND_ROUTREQUEST）。
- Destination address（16 位），路由所需的 Rime 目的址。
- Broadcast counter（8 位），指示目前消息已被传送的次数。
- Broadcast limit（8 位），消息可以被广播的最大次数。

- Broadcast ID（8 位），当前广播消息的 ID。

路由回复消息

- Type（8 位），标识消息类型（COMMAND_ROUTERESPONSE）。
- Destination address（16 位），提供给路由的目的 Rime 地址。
- Battery（16 位）（可选），目的节点的电池水平。

数据传输消息

- Type（8 位），标识消息类型（COMMAND_DATATX）。
- Destination address（16 位），检测数据的目的 Rime 地址。
- Source address（16 位），传输数据的源 Rime 地址。
- Temperature（16 位），待传送的检测到的温度数据。
- Battery（16 位），待传送的电池水平数据。

一个路由表 tsRouteTable 和一个反向表 tsBwsTable 被定义成以下两种数据结构：

- tsBwdTable 结构，只用在路由器中，定义了反向表一个条目的结构，包含

-BrdcstID，用于标识广播消息（8bit）；

-From，接收到路由请求的源设备；

-Dest，所需路由对应的目的地址。

- tsRouteTable 结构，定义了路由表一个条目的结构，包含

-Dest，目的地址（16bit）；

-NextHop，到达目的下一跳（16bit）；

-Battery，电池水平（16bit）；

-Rssi，接收信号强度指示（Received Signal Strength Indication，RSSI）水平（16 位）。

5.3.3.2 软件结构设计

必须开发两个不同的软件应用程序，一个用于发送方，另一个用于路由器和接收方。发送方应用程序负责读取数据、路由和转发数据；接收方应用程序负责接收数据、转发或显示数据。接收方应用程序应该适合路由器和接收器节点，因为这两种类型的节点接收到的数据包是相同类型的。

图 5.16 给出了两个定时器已设置的发送方应用程序流程图。定时器 1 用于设置传感器读数的时间间隔。定时器 2 用于设置路由应答。其路由请求流程图如图 5.17 所示。当需要一个路由发现时，RREQ 消息必须广播给邻居节点，等待 RREP 消息。随后，发送方程序将计算出到达目的最佳路由。计算最佳路由时路由表将被更新，传感器读数作为单播连接被转发到下一跳。这里选择路由所使用的标准是先使用具有较高电池水平的节点，然后选择具有较高的 RSSI 水平的节点。这些标准的逻辑如图 5.17 所示。

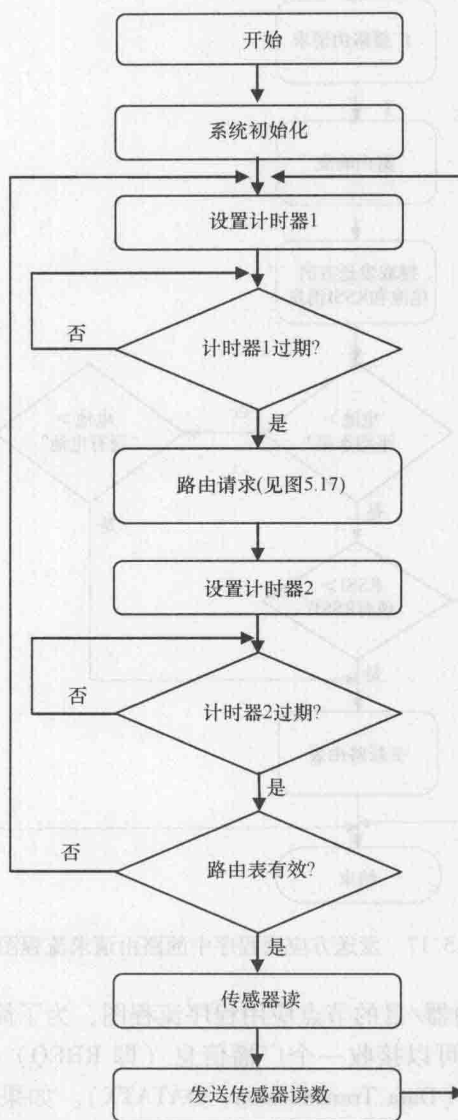


图 5.16　两个定时器已设置的发送方应用程序流程图

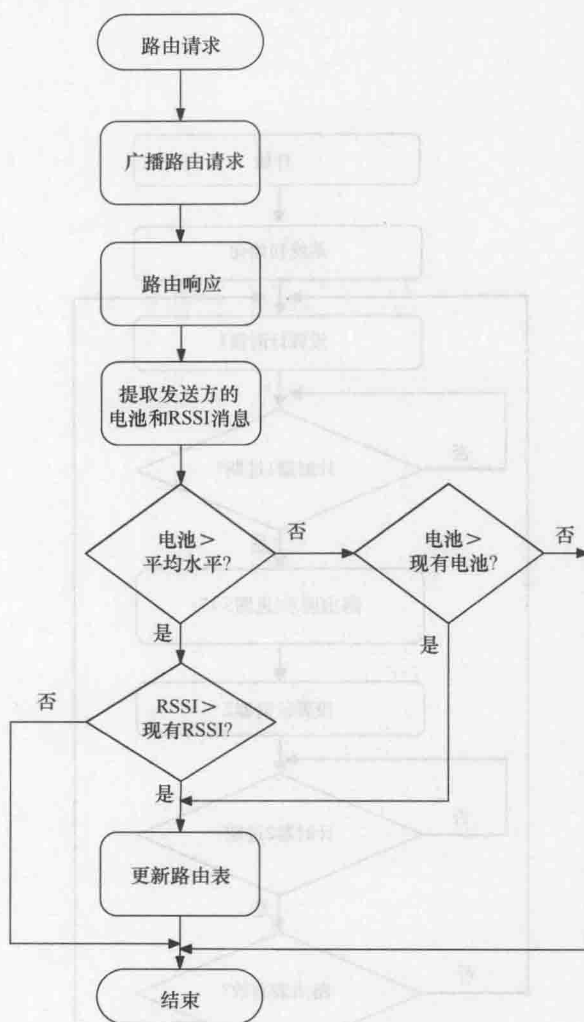


图 5.17　发送方应用程序中的路由请求流程图

图 5.18 给出了路由器/目的节点应用程序流程图，为了简单起见，每个组件的细节被省略了。路由器可以接收一个广播信息（即 RREQ）或两种类型的单播消息：RREP 和数据传输（Data Transmission，DATATX）。如果数据包是 RREQ 的且当前节点不是目的节点时，RREQ 消息将被重新广播。如果当前节点是目的节点，一个 RREP 消息将被送回。如果该数据包是 DATATX 的，该数据包将被转发至其接收器。如果该数据包是 RREP 的，该数据包将被转发至其发送方节点。反向表和路由表应根据需要进行更新。如果广播限制已达到，就必须丢弃当前数据包以避免无用的带宽占用；否则广播计数器将加 1。

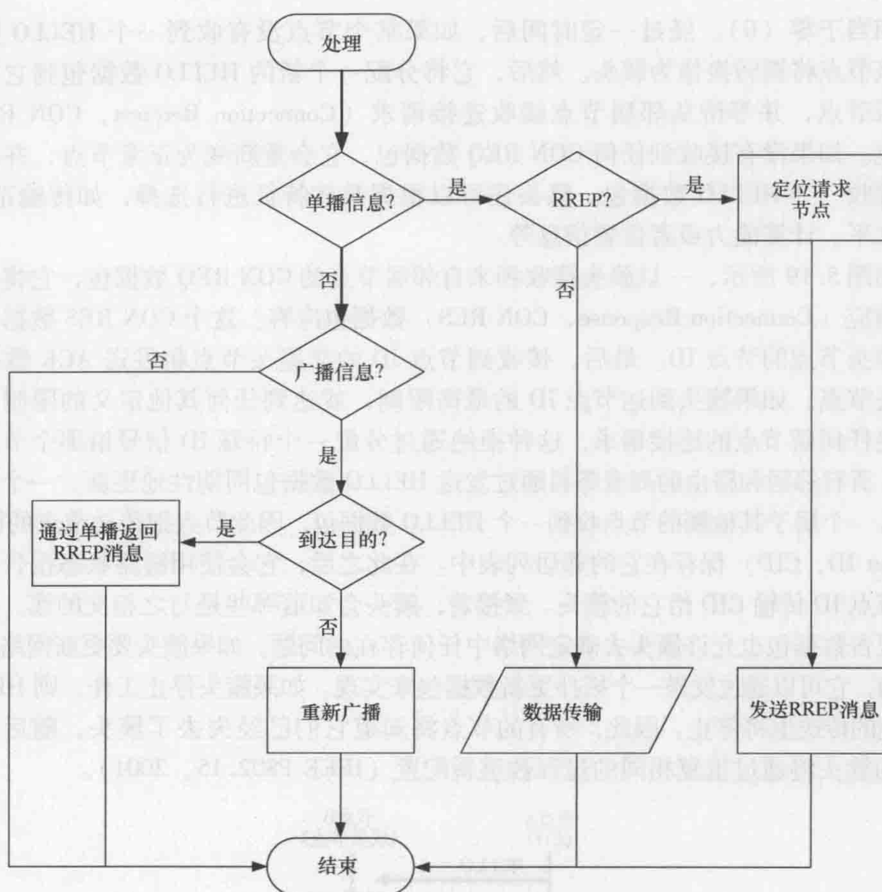


图 5.18　路由器/目的节点应用程序流程图

5.4　簇树路由协议

簇树路由协议（Lee 等，2006）是另一种在 ZigBee 协议栈实现的路由协议，已经被广泛应用于工业领域。它是一个支持网络冗余以实现网络中容错性的自组织协议。簇树路由协议使用数据包协商来形成一个单簇网络或一个多簇网络。簇的形成过程分为两个阶段：选择 WSN 的簇头；随后，WSN 中的非簇头节点加入簇头以形成簇（Ergen，2004）。

5.4.1　单簇网络

单簇网络只包含一个簇头，所有的节点都通过 1 跳连接到这个簇头，网络拓扑结构采用星形拓扑，网络中的每个节点都在等待接收来自充当簇头的节点传送的 HELLO 数据包。HELLO 数据包包括簇头的 MAC 地址和簇头的 ID 号，它在单簇网

络中相当于零（0）。经过一定时间后，如果某个节点没有收到一个 HELLO 数据包，该节点将被转换作为簇头。然后，它将分配一个新的 HELLO 数据包到它的所有邻居节点，并等待从邻居节点接收连接请求（Connection Request，CON REQ）数据包。如果没有接收到任何 CON REQ 数据包，它会重新变为正常节点，并再次等待接收一个 HELLO 数据包。簇头还可以根据某些特征进行选择，如传输范围、能量水平、计算能力或者位置信息等。

如图 5.19 所示，一旦簇头接收到来自邻居节点的 CON REQ 数据包，它将使用连接响应（Connection Response，CON RES）数据包应答。这个 CON RES 数据包包括非簇头节点的节点 ID。最后，接收到节点 ID 的非簇头节点将发送 ACK 数据包到簇头节点。如果簇头到达节点 ID 的最高限制，或达到任何其他定义的限制，它会拒绝任何新节点的连接请求，这种拒绝通过分配一个特殊 ID 信号给那个节点来实现。所有邻居和路由的列表条目通过发送 HELLO 数据包周期性地更新。一个节点可以从一个属于其他簇的节点收到一个 HELLO 数据包，因此节点把传送节点的簇 ID（Cluster ID，CID）保存在它的邻居列表中。在此之后，它会使用链路状态报告中的邻居节点 ID 传输 CID 给它的簇头。紧接着，簇头会知道哪些是与之相交的簇。链路状态报告数据包也允许簇头去确定网络中任何存在的问题。如果簇头要更新网络的拓扑结构，它可以通过发送一个拓扑更新数据包来实现。如果簇头停止工作，则 HELLO 数据包的传送也将停止。因此，所有的节点将知道它们已经失去了簇头，随后，一个新的簇头将通过重复相同的过程被重新配置（IEEE P802.15，2001）。



图 5.19 建立一个簇头和节点之间的链路（IEEE P802.15 2001）

5.4.2 多簇网络

多簇网络由许多单簇构成，如图 5.20 所示。多簇网络需要一个指定的设备（DD，指定设备）来为每个簇头提供一个唯一的簇 ID，并计算出从这个簇到指定设备的最短路由。指定的设备加入网络后，它会充当簇头，并会发送 HELLO 数据包给它的邻居节点。如果簇头收到 HELLO 数据包，它会发送一个 CON REQ 数据包并将加入指定设备形成顶层簇（簇 0）。如果簇头直接连接到指定设备，簇头将

成为具有两个逻辑地址的边界节点。如图5.21所示，如果一个普通节点从指定设备而不是从它的簇头接收到Hello数据包，则它将作为其父节点的边界节点。簇头将发送一个网络连接请求（Network Connection Request，NET CON REQ）数据包来设置与指定设备的连接。随后，边界节点会发送一个CID请求（CID Request，CID REQ）数据包到指定设备。如果指定设备传送一个包含新的CID的CID响应（CID Response，CID RES）数据包给边界节点，边界节点会传送一个网络连接响应（Network Connection Response，NET CON RES）数据包到带有新CID的簇头。此外，簇头将把这个新的CID通知给它的节点。这个过程如图5.21所示。

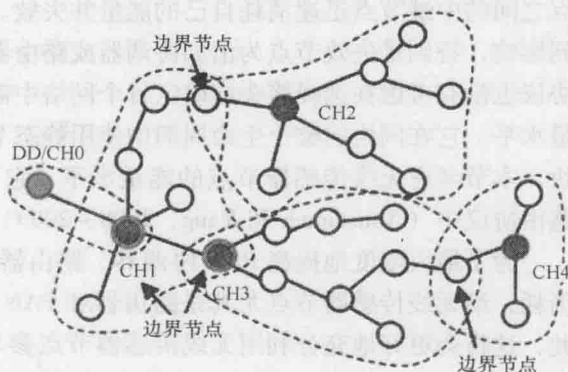


图5.20 多簇网络包含多个单簇（IEEE P802.15，2001）

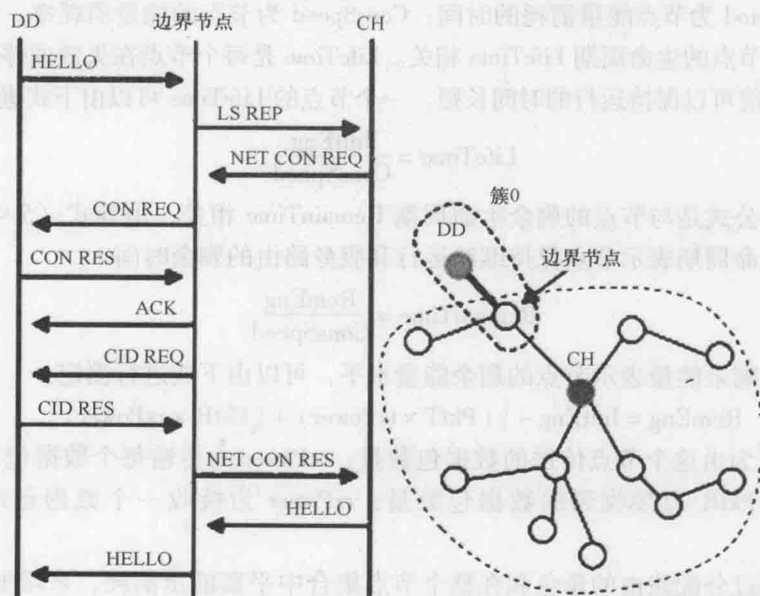


图5.21 通过边界节点连接簇头与指定设备（IEEE P802.15，2001）

5.5 能量感知路由协议

AODV路由协议不是一个能量感知路由协议。AODV路由协议使用相同的路由

来发送所有从源到目的的数据，一直到该路径失效。因此，这条路由上源和目的节点之间的中继节点迅速消耗自己的能量并失效。其结果是整个网络的生命周期将受到影响，特别是失效节点为诸如协调器或路由器时影响更是至关重要的。簇树路由协议也没有考虑在选择簇头或确定每个网络中需要的簇数目时无线传感器节点的能量水平。它在网络的整个生命周期中使用静态节点充当簇头，使得这些节点失效很快。本节考虑无线传感器节点的能量水平，它可以应用在 AODV 路由协议和簇树路由协议中（Abusaimeh 和 Yang，2008～2009）。

为了最大限度地提高 PAN 协调器、路由器及整个网络的生命周期，平衡能量消耗，给无线传感器节点尤其是路由器和 PAN 协调器分配路由职责是必需的。因此，这将会更好地充分利用无线传感器节点参与通信过程，共享数据传输（Abusaimeh 和 Yang，2008）。首先，提出 WSN 的能量模型。这种能量模型包括几个公式。第 1 个公式与每个传感器节点的能量消耗率相关，可以被定义为

$$\text{ConsSpeed} = \frac{\text{InitEng} - \text{RemEng}}{\text{TimePeriod}} \tag{5.2}$$

式中，RemEng 为该节点的当前能量水平；InitEng 为该节点加入网络时的初始能量水平；TimePeriod 为节点能量消耗的时间；ConsSpeed 为节点的能量消耗率。第 2 个公式是与每个节点的生命周期 LifeTime 相关。LifeTime 是每个节点在失效或停止发射和接收信号之前可以保持运行的时间长短。一个节点的 LifeTime 可以由下式进行测定：

$$\text{LifeTime} = \frac{\text{InitEng}}{\text{ConsSpeed}} \tag{5.3}$$

第 3 个公式是与节点的剩余生命周期 RemainTime 相关，由等式（5.4）描述。这个剩余生命周期表示节点保持继续运行和服务路由的剩余时间。

$$\text{RemainTime} = \frac{\text{RemEng}}{\text{ConsSpeed}} \tag{5.4}$$

节点的剩余能量表示节点的剩余能量水平，可以由下式进行测定：

$$\text{RemEng} = \text{InitEng} - [(\text{PktT} \times \text{txPower}) + (\text{PktR} \times \text{rxPower})] \tag{5.5}$$

式中，PktT 为由这个节点传送的数据包数量；txPower 为传输每个数据包所需要的传输能量；PktR 为接收到的数据包数量；rxPower 为接收一个数据包所消耗的能量。

可以通过分配路由的角色和在整个节点集合中平衡能量消耗，来增加 WSN 的生命周期。可以通过同时考虑无线传感器节点电池的能量水平变化与路由探索过程和数据包转发过程，来实现生命周期的最大化。在能量感知路由协议中，大多数节点将作为源节点和目的节点之间的中继节点。如果通往目的节点路由中的某个中继节点具有较低的能量水平或更高的能量消耗率，则将建立一条新的路由，建立一条新的路由的能量成本 EstRouteCost 可以通过下式：

$$\text{EstRouteCost} = \text{HopsNo} \times \text{txPower} \times \text{Time} \tag{5.6}$$

式中，HopsNo 为源和目的节点之间的跳数；txPower 为用于一个数据包的传输能量；Time 为传送这些发现数据包所需的时间。因为建立一个新路由需要的时间很短，所以建立一个新路由的整个能源成本可能是微不足道的。

此外，能量感知路由将致力于保持大多数节点在其最大生命周期上运行。具有高能量消耗率和短剩余生命周期的每个节点应关闭一段时间。高能量消耗率是由该节点的能量消耗率与其他节点相比较来确定的。关闭一个节点将使能量感知路由协议选择代替节点或改变整个到目的节点的路由。重复这个过程能够在大多数节点之间分配路由角色，因此从整体上平衡了网络能量消耗。

现有的能量感知路由协议（如 AODV 路由协议或簇树路由协议等）还需要额外的步骤。AODV 能量感知路由协议的步骤如图 5.22 所示。这些步骤如下：

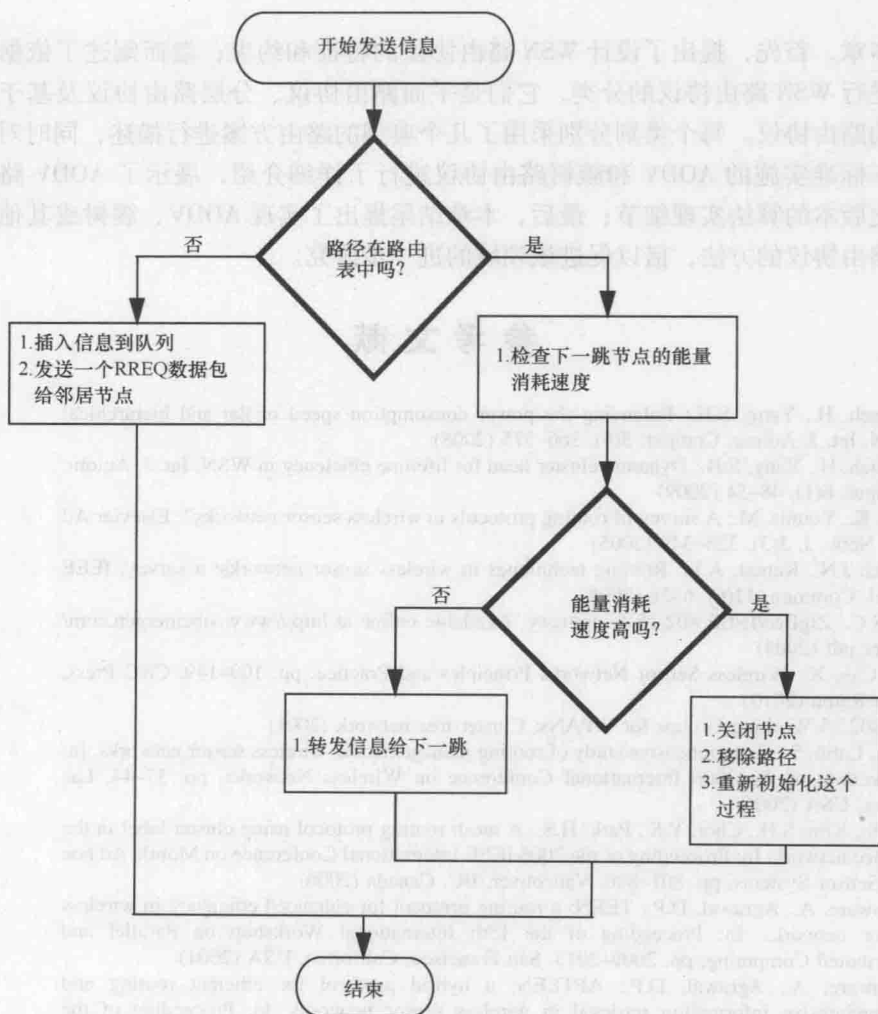


图 5.22 AODV 能量感知路由协议的步骤

步骤 1。如果一个传感器节点需要发送一个消息，它必须检查它的路由表来找到一条通往目的节点的路由。因此，如果在路由表中可以找到一个路由，它将该消息转发到下一个节点。否则，该消息将被保存在队列中，源节点将发送 RREQ 数据包到其邻居节点启动路由发现过程。

步骤 2。将消息转发到下一跳之前，检查下一跳的能量消耗率。

步骤 3。如果能量消耗率高，那么下一跳将被关闭一段规定的时间。该路由将从路由表中移除，这将导致在源节点再次启动路由发现过程，寻找到达目的节点的新路由。

5.6 小结

本章，首先，提出了设计 WSN 路由协议的特征和约束；继而阐述了依据网络结构进行 WSN 路由协议的分类，它们是平面路由协议、分层路由协议及基于地理位置的路由协议。每个类别分别采用了几个典型的路由方案进行描述，同时对基于 ZigBee 标准实施的 AODV 和簇树路由协议进行了详细介绍，展示了 AODV 路由协议简化版本的算法实现细节；最后，本章结尾提出了实现 AODV、簇树或其他能量感知路由协议的方法，借以促进该领域的进一步研究。

参考文献

Abusaimeh, H., Yang, S.H.: Balancing the power consumption speed in flat and hierarchical WSN. Int. J. Autom. Comput. **5**(4), 366–375 (2008)

Abusaimeh, H., Yang, S.H.: Dynamic cluster head for lifetime efficiency in WSN. Int. J. Autom. Comput. **6**(1), 48–54 (2009)

Akkaya, K., Younis, M.: A survey of routing protocols in wireless sensor networks". Elsevier Ad Hoc Netw. J. **3**(3), 325–349 (2005)

Al-karaki, J.N., Kamal, A.E.: Routing techniques in wireless sensor networks: a survey. IEEE Wirel. Commun. **11**(6), 6–28 (2004)

Ergen, S.C.: ZigBee/IEEE 802.15.4 summary. Available online at http://www.sinemergen.com/zigbee.pdf (2004)

Hu, F., Cao, X.: Wireless Sensor Networks Principles and Practice, pp. 109–149. CRC Press, Boca Raton (2010)

IEEE P802.15 Working Groups for WPANs: Cluster tree network (2001)

Jolly, V., Latifi, S.: Comprehensive study of routing management in wireless sensor networks. In: Proceeding of the 2006 International Conference on Wireless Networks, pp. 37–44. Las Vegas, USA (2006)

Lee, K.K., Kim, S.H., Choi, Y.S., Park, H.S.: A mesh routing protocol using cluster label in the ZigBee network. In: Proceeding of the 2006 IEEE International Conference on Mobile Ad hoc and Sensor Systems, pp. 801–806. Vancouver, BC, Canada (2006)

Manjeshware, A., Agrawal, D.P.: TEEN: a routing protocol for enhanced efficiency in wireless sensor networks. In: Proceeding of the 15th International Workshop on Parallel and Distributed Computing, pp. 2009–2015. San Francisco, California, USA (2001)

Manjeshware, A., Agrawal, D.P.: APTEEN: a hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks. In: Proceeding of the

International Workshop on Parallel and Distributed Computing, pp. 195–202, Ft. Laudeerdale, FL, USA (2002)
Perkins C.E., Royer, E.M.: Ad-hoc on-demand distance vector routing, The mobile Ad-hoc network (MANET) working group IETF, pp. 173–219 (2003)
Vidhyapriya, R., Vanathi, P.T.: Conserving energy in wireless sensor networks. IEEE Potentials **26**(5), 37–42 (2007)
Xu, Y., Heidemann, J.: Geography-informed energy conservation for ad hoc routing. In: International conference on mobile computing and networking, pp. 70–84, Rome, Italy (2001)
Yu, Y., Govindan, R., Estrin, D: Geographical and energy-aware routing: a recursive data dissemination protocol for wireless sensor networks, UCLA computer science department technical report, UCLA-CSD TR-01-0023, pp. 1–11 (2001)



第 6 章 汇聚节点位置的优化布局

关键词： 汇聚节点位置布局　静态移动　动态汇聚节点　进化计算

6.1 引言

虽然 WSN 拥有像星形、环形、网状或者是树形网络等各种网络拓扑结构，但是来自于 WSN 中每个传感器的信号会经由几个汇聚节点传输到互联网或者其他终端。一个汇聚节点是一个连接到普通传感器上的指定设备，它比普通的传感器功率更大并且通过它可以将多个终端用户桥接成一个 WSN。汇聚节点可以被设计为一个从网络接收数据的笔记本计算机，或者是一个更小的专用的并且能够提供网关功能的微型控制器。如图 6.1 所示，每个传感器节点都具有收集数据并将数据路由到其他节点和终端用户的能力。数据通过汇聚节点的路由返回给终端用户。

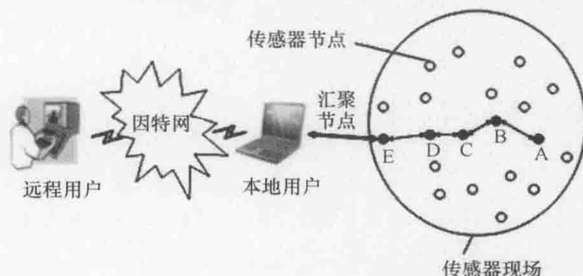


图 6.1　分散传感器节点中的汇聚节点

根据不同的应用需求，可能会有一个以上的汇聚节点同时工作在传感器网络上。图 6.2 给出了分散传感器节点中的多汇聚节点，传感器节点 B 参与到了 X 和 Y 这两个汇聚节点之间的通信。如图 6.2 所示，当两个汇聚节点被部署后，传感器节点 A 是跳转到汇聚节点 Y 的最近一个节点，并且经过多跳到汇聚节点 X。因此，采用两个汇聚节点代替一个汇聚节点时，传感器节点 A 可以通过更少的跳数和更低的功率将信号传输到汇聚节点。众所周知，当一条信息从任意一个传感器节点到它最近的汇聚节点时，其消耗的功率与该信息传递的跳数呈正比。采用多个汇聚节点可有效减少每次信息传递时的功率消耗。当汇聚节点的数量增加时，传感器节点到汇聚节点的路径长度缩短，传感器节点的寿命会增加。然而，由于汇聚节点的成本要高于传感器节点，因此汇聚节点的数量在部署时会加以限制。此外，在某些情况下，采用多汇聚节点在物理上是不能实现的。

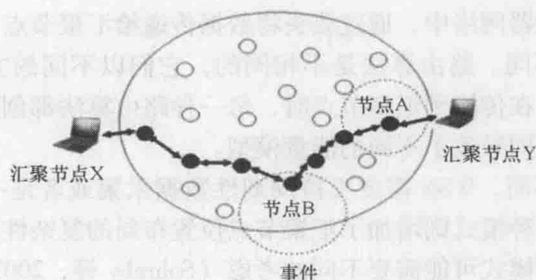


图6.2 分散传感器节点中的多汇聚节点

汇聚节点的位置布局可以影响网络的性能。Heinzelman 等人（2000）通过实验结果表明，单跳到汇聚节点的传感器节点要比传感器网络中的其他节点更快地耗尽它们的能量。这是因为单跳到汇聚节点的传感器节点除了需要发送自身的节点信息外，还需要转发来自于其他节点的信息。这些距离汇聚节点较近的传感器节点的工作量，要大于那些距离汇聚节点较远的传感器节点。因此，这些传感器节点会很快耗尽它们的能量并结束它们的使用寿命。如果汇聚节点周围大量的传感器节点消亡，那么它也就变得无效，其他未消亡的传感器节点则不能经由这些已经消亡的传感器与汇聚节点进行通信，传感器网络也就变得无效了。

6.2 汇聚节点位置布局的挑战

在 WSN 中优化汇聚节点的位置布局存在着大量的挑战。它包含一个巨大的并且是有限的解决空间。在这些空间中包含大量的参数、不同的路由算法、不同的应用需求，涉及大量的传感器节点和不同的传感器节点性能。

● 巨大的并且是有限的解决空间。汇聚节点可以在环境中任意位置进行位置布局，并且不胜枚举（Oyman 和 Ersoy，2004）。当没有应用限制时，拥有大量的解决方案。

● 涉及大量的传感器。传感器网络可能包含上千个传感器节点。大量传感器节点参与导致汇聚节点面临着非决定性多项式时间完全问题（NP-complete）。

● 动态拓扑结构的变化。被部署后的传感器节点可能由于制造缺陷或者是能量耗尽而导致失败，因此就需要改变传感器网络的拓扑结构和汇聚节点的位置。

● 不同的节点性能。传感器节点不是完全相同的，如有些节点采用可变发送器而有些不是。在这种情况下，最大限度地减小 WSN 中各个传感器节点与固定发射器和各个通信子网之间的距离能够更好地减少能量的消耗，但是在固定的通信范围内只有一个传感器节点则不能节省能量。

● 网络结构的不同。有两种典型的传感器网络体系结构：平面结构和层次结构。平面结构的传感器网络通过在网络中的中间节点以一种多跳的方式传播数据；

而在层次结构的传感器网络中，通过簇头将数据传递给汇聚节点。

- 路由算法的不同。路由算法是不相同的，它们以不同的方法来优化传感器网络中的数据传输。在传输到汇聚节点时，每一种路由算法都创建了一类独特的数据传输结构。这种不同导致了不同的能量模型。
- 采集模式的不同。WSN 需要支持周期性数据采集或者是一个事件驱动模式的操作。同时支持两种模式则增加了汇聚节点位置布局的复杂性。另一方面，选择优化特定数据的采集模式可能需要不同的考虑（Sohraby 等，2007）。

6.3 汇聚节点位置布局方法的分类

在大部分有关汇聚节点位置布局的研究中，都集中在汇聚节点的位置选择上，这可能会影响各种性能指标，如能量消耗、延迟和吞吐量等。它们注重网络结构的质量标准，如距离和网络连接，和/或基础的拓扑结构分析。因此，这里将它定义为静态方法。然而，动态调整汇聚节点的位置可以进一步提高 WSN 的可靠性，因为对汇聚节点最初位置的优化会随着网络的运行而变得无效，这都是由网络状态的变化或者是外部因素的改变所带来的。例如，在目标跟踪的应用中，对于紧邻已被监测到的目标节点和通信量高的目标节点的汇聚节点进行重新位置布局是合理的。这里将它定义为动态方法。

6.3.1 汇聚节点的静态位置布局

在静态汇聚节点的位置布局中，汇聚节点没有移动的能力。它的位置在整个网络运行的生命周期中是固定的。研究人员对网络设置时间的优化问题及用于单个或者多个汇聚节点在 WSN 中的位置布局做了大量的工作。在已经公开的研究成果中，一般根据假设条件、网络模型、网络的状态信息和指标的优化进行分类。

延长网络的生命周期是静态汇聚节点位置布局的关键目标。汇聚节点位置布局的多个变种已经被广泛研究（Akkaya 等，2007）。这种差异或者是由于网络生命周期的定义、网络运行模式或者是包含在优化目标之内的网络状态参数引起的。虽然有些用户认为网络寿命是直到第一个传感器节点失效的时间，但是一些其他的用户用部署的传感器的失效比率作为网络生命周期的指示。其他的研究致力于通过减少传感器采集数据总体能量的消耗来延长网络的生命周期。

网络拓扑结构和系统模型同样被认为是一个用来鉴别因素。在平面网络拓扑结构中，传感器是均匀的，具有相同的初始能量，并且通常形成多路由来中继它们的数据到汇聚节点。在分层拓扑结构中，传感器节点根据指定的簇头进行分簇。在这种情况下，汇聚节点位置布局问题的范围缩小到簇头间的网络。图 6.3 给出了两层结构的 WSN。在网络中，用 SN 表示传感器节点，AN 表示作为簇头的应用节点，

BS表示基站，其他的是汇聚节点。汇聚节点所选择的位置应尽可能减小簇头结点和汇聚节点间的最大距离，或者是减小簇头结点到汇聚节点间数据传输的能量消耗。

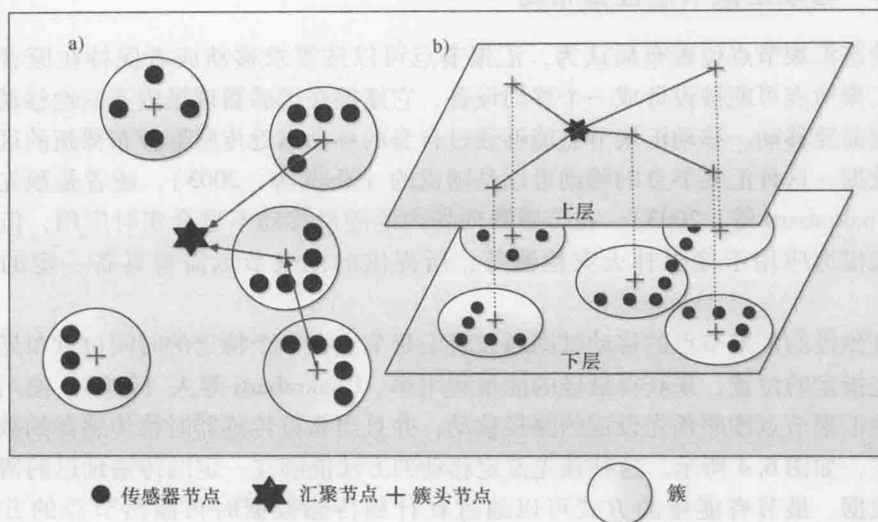


图6.3 两层结构的WSN
a）物理层视图 b）逻辑层视图

6.3.2 动态汇聚节点位置布局

静态汇聚节点位置布局不考虑网络运行过程中的动态变化，因此一旦汇聚节点被部署在初始位置后就不会再移动。动态变化的例子包括，基于监控事件的交通模式的变化；节点之间许多不平衡负载引起的瓶颈；应用程序的要求会随着时间而改变；现有的网络资源可能会由于某些节点的能量消耗而发生变化（Akkaya等，2007）。

当网络运行时，动态的位置布局汇聚节点可以进一步提高网络的性能。例如，在目标跟踪的应用中，让汇聚节点与有害的目标节点保持一定距离是明智的，它们之间应该保持一个安全的距离。在灾害管理应用中，传感器可以检测到火灾、建筑物倒塌、煤气泄漏等。上述事件，一旦人员近距离接触将会非常危险。另一个例子是，汇聚节点周围的许多传感器节点由于它们的电池耗尽变得失效了。这时，汇聚节点需要重新定位，保证与数据源方便、可靠的连接。Vincze等人（2006）建议当事件发生时，在基于事件驱动的传感器网络中的汇聚节点应该进行自适应地重新位置布局。Akkaya等人（2005）提出了三步法：汇聚节点何时应该重新定位；定位在哪里；以及如何将数据路由到汇聚节点的新的位置。Akkaya等人（2007）分别根据能量消耗、数据传输中继和汇聚节点的安全提出了能够提高网络性能的汇聚

节点动态重新位置布局的三个启发式案例。它们是为了提高网络寿命、提高时延受限流量的及时性，以及保护汇聚节点。

6.3.3 移动汇聚节点位置布局

动态汇聚节点位置布局认为，汇聚节点可以按需求移动或者保持在原有位置上。汇聚节点可能被设计成一个移动设备，它能够在传感器现场内不断地移动而不是根据需要移动。移动汇聚节点能够通过自身的移动靠近传感器分布稀疏的区域去采集数据。这种汇聚节点的移动可以是随机的（Shah 等，2003），或者是预先设定的（Chakrabarti 等，2003）。在传感器现场内的随机移动不适合实时应用，但是可以大规模地应用于像森林火灾检测等，所提供的汇聚节点需要具备一定的飞行能力。

可预设的汇聚节点的移动试图通过将汇聚节点在一个特定的时间位置布局在一个预先指定的位置，来获得最佳的能量利用率。Chakrabarti 等人（2003）使用一个移动的汇聚节点按照预先设定的路径移动，并且当靠近传感器时将传感器的数据采集过来，如图 6.4 所示。这种预先设定移动的方法能够在一定的传输延迟的情况下收集数据。最节省能量的方式可以通过在计划传输数据时再激活节点的方式来实现。

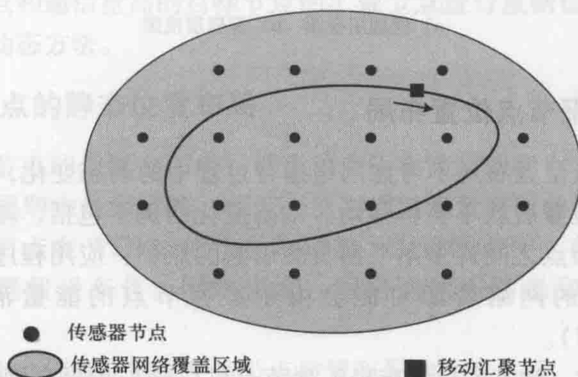


图 6.4　一个移动汇聚节点的传感器网络

6.4 静态多汇聚节点的位置布局优化

6.4.1 系统假设

这里限制 WSN 为网状拓扑结构，如图 6.5 所示。为简单起见，在建立 WSN 系统模型时作以下假设：

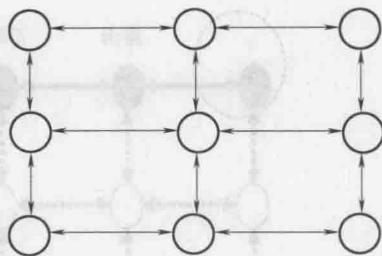


图6.5 网状拓扑结构的WSN

- 所有的传感器节点都是固定的，并且位于一个大小相等的二维正方形网格单元内；
- 多个汇聚节点被固定在网格之内；
- 数据传输和接收是主要的能量消耗活动；
- 所有的传感器节点具有相同的初始能量；
- 每个传感器节点的传输范围是固定的，并且等于网格中两个相邻节点的距离，即每一跳是一个网格单元的边长；
- 传感器节点与汇聚节点通过多跳沿最短路径发送数据；
- 汇聚节点的个数是固定的，并且预先知道；
- 汇聚节点只能位于网格内的某个位置，称为可行性站点；
- 在传感器节点上传输一位数据和接收一位数据在能量消耗上是相同的。

以前，传感器网络表示为图 G（V, E）。其中，V为传感器节点的顶点；边 E 为两个相邻节点（i, j）之间的单跳连接。考虑到 WSN 中的网状拓扑结构，一个传感器节点 i 可以与它自身四个方向（左、右、上和下）上的节点直接进行通信。如果传感器节点不是通过单跳与汇聚节点进行连接的，那么这个传感器节点上产生的数据包需要经过多跳中继到汇聚节点上。

这里采用 Wang 等人（2005）工作中提出的符号和公式描述每个传感器节点的能量消耗，并且将其扩展到多静态汇聚节点的情况。

- e 为发送或者接收一位数据消耗的能量（J/bit）；
- e_0为每个节点的初始能量（J）减去节点操作所需能量的阈值；
- r 为数据包产生的速率（bit/s），对同构的传感器来说，所有传感器节点的 r 是相同的；
- C_i^k为从节点 i 到汇聚节点 k 之间接收和发送数据的能量消耗（J/s）；
- z 为网络生命周期（s）；
- z_{ij}为节点 i 分配到汇聚节点 k_j的生命周期（s）。

6.4.2 简化路由协议

如图6.6所示，这里分析一个网状拓扑结构 WSN 的简化路由协议。

当一个传感器节点与汇聚节点位于同一水平或者垂直线上时，将会选取唯一一条由传感器节点到汇聚节点的最短路径；否则，选取以传感器节点和汇聚节点作为对角的矩形的两侧直角边为路径。这两条路径被采用的几率是相同的。

图6.6中有三种情况。在图6.6a、b中，传输一个数据包从节点 i 到汇聚节点需要两跳。在图6.6c中，在两条对称路径中传输一个数据包需要四跳。

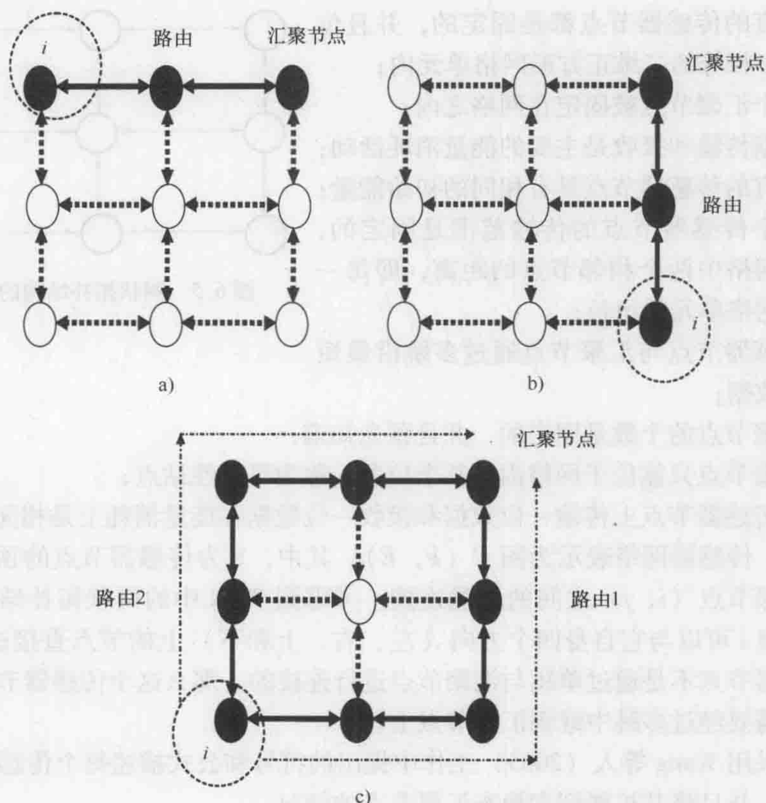


图 6.6 网状拓扑结构 WSN 的简化路由协议

6.4.3 能耗模型

继续采用以上符号（Wang 等，2005），每一个节点位置用行和列数据(x，y)的有序节点对来表示。其中，$x=0$，1，…，$L-1$；$y=0$，1，…，$L-1$；L 为网格中的列和行数。一对围绕与汇聚节点的行和列相关的节点的水平和垂直的虚线被绘制出来，这些线将传感器划分成 9 个区域（见图 6.7）：左上（UL），右上（UR），左下（LL），右下（LR），正上（VA），正下（VB），正左（HL），正右（HR）和汇聚节点 k 自身所在位置。Wang 等人（2005）给出如式（6.1）的公式来计算节点 i 的能量消耗。

以节点 i 在 UR 子集为例，节点 i 连续成功地传输自身产生的数据包到节点 j_2 和 j_4，节点 j_2 和 j_4 中继这些数据包到汇聚节点 k。另外，节点 i 接收节点 j_1 和 j_3 所产生数据包的一半，另一半数据包产生于节点 l_1 和 l_2。然后，节点 i 转发由节点 j_3 和 l_2 所产生的数据包到节点 j_2，j_1 和 l_1 产生的数据包转发到节点 j_4。总之，节点 i 接收数据包的速率是 $2r$，发生数据包的速率是 $3r$，因此能量消耗为 $C_i^k=5re$。

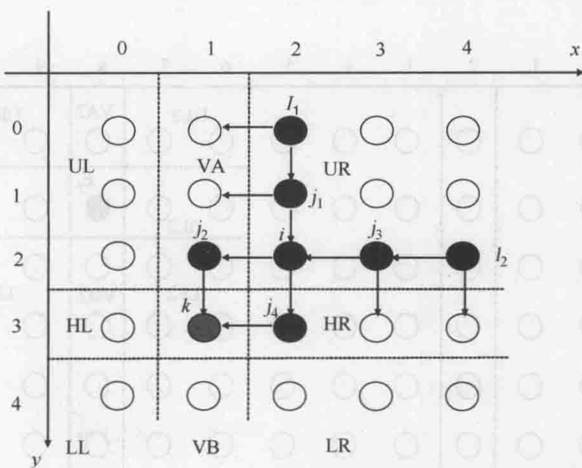


图 6.7　在节点 i 上的数据流的接收和发送（Wang 等，2005）

$$c_i^k = \begin{cases} er[(x+1)(1+L)-1] & i \in \text{HL} \\ er[(L-x)(1+L)-1] & i \in \text{HR} \\ er[(y+1)(1+L)-1] & i \in \text{VA} \\ er[(L-y)(1+L)-1] & i \in \text{VB} \\ er(1+x+y) & i \in \text{UL} \\ er(L-x+y) & i \in \text{UR} \\ er(L+x-y) & i \in \text{LL} \\ er(2L-x-y-1) & i \in \text{LR} \\ er & i \in K \end{cases} \tag{6.1}$$

如果有多个汇聚节点在传感器的现场，传感器的现场可以进一步划分。图 6.8 给出了拥有两个汇聚节点（k_1 和 k_2）的传感器现场的划分。子集划分为 UL1、UR1、LL1、LR1、VA1、VB1、HL1、HR1 和 UL2、UR2、LL2、LR2、VA2、VB2、HL2、HR2，根据两个汇聚节点的位置一些子集将会重叠。计算能量消耗的公式为式（6.1），该公式同样适用于图 6.8 所示的多汇聚节点的情况。如果所有传感器节点被分配到离它们最近的汇聚节点并且没有重复分配的话，每一个节点会分配给一个且仅分配给一个汇聚节点。

6.4.4　多汇聚节点的位置布局优化

假设传感器网络有 N 个汇聚节点 k_1，k_2，…，k_N，被分配给汇聚节点 k_j 的任意传感器节点 i 的生命周期可以由下式给出：

$$z_{ij} = \frac{e_0}{c_i^{k_j}}$$

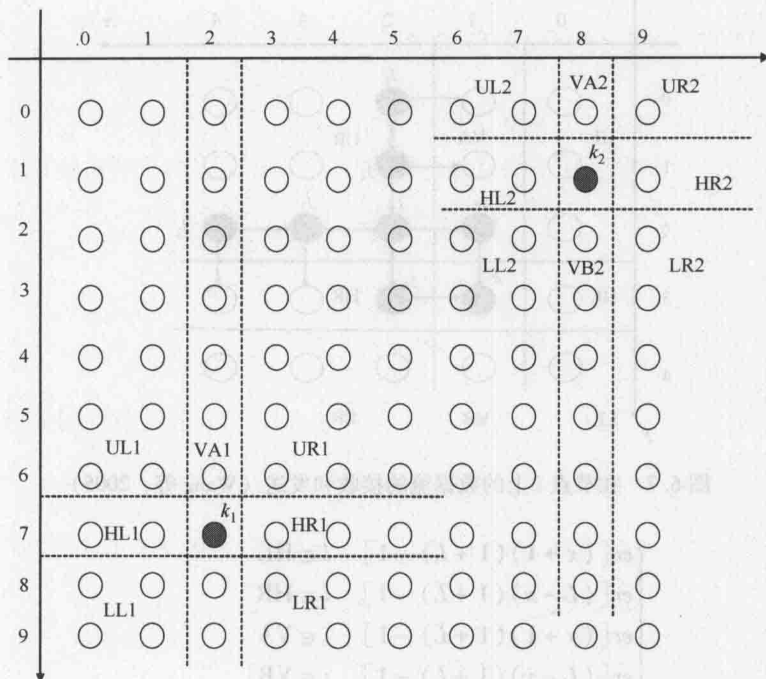


图 6.8 拥有两个汇聚节点（k_1 和 k_2）的传感器现场划分

被分配到最近的汇聚节点的传感器节点 i 的生命周期用下式给出：

$$\max\left(\frac{e_0}{c_i^{k_j}}\right) \quad j=1,2,\cdots,N$$

传感器网络的生命周期可以被定义为直到传感器网络第 1 个节点电池容量耗尽的时间，即

$$\min_i\left\{\max_j\left(\frac{e_0}{c_i^{k_j}}\right)\right\}$$

为了使传感器网络的生命周期最大化，所有传感器节点的最短生命周期应该通过优化多个汇聚节点的位置而最大化。下面多个汇聚节点的最优位置布局的目标给出（Yang，2006）：

$$z=\max_{k_1,k_2,\cdots,k_N}\left\{\min_i\left\{\max_j\left(\frac{e_0}{c_i^{k_j}}\right)\right\}\right\} \quad i=0,1,\cdots,L \tag{6.2}$$

在传感器现场，汇聚节点不能放置在任何有障碍物的位置，位置布局可以定义成上面带有约束的优化问题，ϕ 为障碍物集，有

$$k_1,k_2,\cdots,k_N \notin \phi \tag{6.3}$$

6.5 位置布局优化问题的求解

多种优化方法可以用于解决优化位置布局问题，如式（6.1）~式（6.3）。由于在上述优化中存在多个变量的特性，因此大部分进化算法能够被应用到解决位置布局问题当中去（Yang，2006；Alageswaran 等，2012）。Yang（2006）提出利用遗传算法进行优化位置布局问题，具体有下列三个定义的描述：

- 用染色体来表示相应的运算操作；
- 将这种表示定义为一种适应度函数；
- 存在一组操作算子，如交叉、变异和繁殖。

在式（6.2）给出的目标函数中被优化的变量是 N 个汇聚节点的坐标，即 N 组整型坐标变量。

$$(i_a, j_a) \quad a = (1, 2, \cdots, N) \tag{6.4}$$

染色体被表示为如下所示的长度为 $2N$（汇聚节点数量的两倍）的整型字符串：

$$i_1 \quad j_1 \quad i_2 \quad j_2 \quad \cdots \quad i_N \quad j_N \tag{6.5}$$

这里

$$\begin{cases} (i_a, j_a) \neq (i_b, j_b) & \text{当 } a \neq b \quad (6.6) \\ (i_a, j_a) \notin \phi & a = (1, 2, \cdots, N) \quad (6.7) \end{cases}$$

式（6.6）表示两个不同的汇聚节点不能位于同一个位置上，式（6.7）表示汇聚节点不能与障碍物位置布局在同一个位置上。

式（6.2）所示的遗传算法适应度函数被选作目标函数。

$$f_{\text{fitness}} = \min_j \left\{ \max_i \left(\frac{e_0}{c_i^{k_j}} \right) \right\} \tag{6.8}$$

对于具有 N 个汇聚节点的所有可能的组合，通过式（6.8）可以获得适应度函数期望值的最大值。遗传算法的三个算子——交叉、变异、繁殖，被用来在式（6.6）和式（6.7）做满意度函数约束下的如式（6.5）的染色体的更新。

以下是一个简单的仿真模拟实例。在一个 8×8 的传感器网络中，设计了两个汇聚节点，但这两个汇聚节点不允许在点（1，1）、（5，5）和（6，6）上进行位置布局。在初始阶段，这两个汇聚节点是随机选择的，所以遗传算法从描述一些优化位置布局问题随机解的几条染色体开始进化。遗传算法参数选择的概率分别为，变异概率为 0.08，交叉概率为 0.6，染色体种群规模为 20。8×8 传感器网络的参数值为 $r = 1\text{bit/s}$，$e = 0.62\mu\text{J/bit}$，$e_0 = 1.35\text{J}$。搜索的结果表明，左上角（0，0）和右下角（7，7）是两个汇聚节点的最优位置布局位置。这一结果与 Wang 等人（2005）所研究的移动汇聚节点的结果是一致的。

6.6 小结

本章仅考虑利用简单的路由算法来优化多个汇聚节点位置布局的问题。如果一些其他的路由算法被应用到传感器网络中，则系统模型可能会变得更加复杂。6.4.1节所作的假设也是简化的，特别是假设所有的传感器节点是固定的，并且位于一个由相同大小元素所组成的二维正方形网格中；在网格中两个相邻节点的每个传感器节点传输的范围是固定的，距离是相等的。这两个假设使得系统模型变得简单，但不容易实现，因为传感器节点是随机分布的，并且它们可能有不同的通信范围。同样假设汇聚节点的数量是固定的，并且预先知道是多少。如果这个假设不真实，汇聚节点的数目就必须作为一个额外的优化变量被导入优化中。不过，本章提出的方法和对搜索问题的建模适用于任何复杂的汇聚节点位置布局问题。

参考文献

Akkaya, K., Younis, M., Bangad, M.: Sink repositioning for enhanced performance in wireless sensor networks. Comput. Netw. **49**(4), 512–534 (2005)

Akkaya, K., Younis, M., Youssef, W.: Positioning of base stations in wireless sensor networks. IEEE Commun. Mag. **45**(4), 96–102 (2007)

Alageswaran, R., Usha, R., Gayathridevi, R., Kiruthika, G.: Design and implementation of dynamic sink node placement using particle swarm optimization for life time maximization of WSN applications. International conference on advances in engineering, science and management. Nagapattinam, Tamil Nadu, pp. 552–555 (2012)

Chakrabarti, A., Sabharwal, A.,and Aazhang, B.: Using predictable observer mobility for power efficient design of sensor networks. Information Processing in Sensor Networks, Lecture Notes in Computer Science, vol. 2634, pp. 129–145 (2003)

Heinzelman, W.R., Chandrakasan, A., Balakrishnan, H.: Energy-efficient communication protocol for wireless microsensor networks. In: Proceedings of the 33rd annual Hawaii International Conference on System Sciences, p. 10, (2000)

Oyman, E. I., Ersoy, C.: 2004 IEEE international conference on communications, vol. 6, pp. 3663–3667

Pan, J., Cai, L., Hou, Y.T., Shi, Y., Shen, S.X.: Optimal base-station locations in two-tiered wireless sensor networks. IEEE Trans. Mob. Comput. **4**(5), 458–473 (2005)

Shah, R.C., Roy, S., Jain, S., Brunette, W.: Data MULEs: modeling and analysis of a three-tier architecture for sparse sensor networks,". Ad Hoc Netw. **1**(9), 215–233 (2003)

Sohraby, K., Minoli, D., Znati, T.F.: Wireless sensor networks: technology, protocols, and applications. Wiley, New York (2007)

Vincze, Z., Vass, D., Vida, R., and Vidács, A.: Adaptive sink mobility in event-driven clustered single-hop wireless sensor networks. In: Proceedings of the 6th International Network Conference, Plymouth, UK, pp. 315–322 (2006)

Wang, Z. M., Basagni, S., Melachrinoudis, E., Petrioli, C.: Exploiting sink mobility for maximizing sensor networks lifetime. In: Proceedings of the 38th Annual Hawaii International Conference on System Sciences, p. 287a (2005)

Yang, L.: Determining sink node locations in wireless sensor networks. IEEE international conference on systems, man and cybernetics, pp. 3400–3404 (2006)

第 7 章　无线传感器网络与 IEEE 802.11b 系统的互扰抑制

关键词：互扰　能量监测　互扰抑制　IEEE 802.15.4　IEEE 802.11b　Wi-Fi

7.1　引言

快速发展的无线技术通过消除有线技术的缺陷，使许多应用发生了显著变化，但是无线互扰严重制约了无线设备的发展。由于无线通信媒介可能完全处于互扰源的互扰范围内，所以和有线系统不同，无线系统对互扰不能进行有效的抑制。流行的2.4GHz ISM 频段的无线产品主要有 Wi-Fi、蓝牙、ZigBee、微波炉、无绳电话等（Thonet 等，2008）。由于这些主要是电子消费产品，所以用户经常会同时使用两个或多个这类电子产品。因此，如果多个无线产品同时工作在相同的频段，那么产品的性能就会受到影响。

IEEE 802.15.4 标准作为低数据率、低成本的无线解决方案，广泛应用在 WSN 这样的无线个人局域网中。IEEE 802.15.4 标准支持构建低成本的无线连接，从而可以在家居、商业和工业中实现监视和控制功能。由于 WSN 具有可移动性并可广泛部署，所以会出现不同的无线系统在相同的地点同时工作的情况，这会使 IEEE 802.15.4 WSN 之间的无线链路极易受到互扰。由于 IEEE 802.15.4 WSN 具有传输功率低（典型的为 1mW）和频段窄（每个信道为 2MHz）的特点，所以其无线传输容易受到其他强无线系统的互扰。在许多实际应用中，IEEE 802.15.4 WSN 和 IEEE 802.11b Wi-Fi 系统可能在同一区域同时工作。最近的理论分析和一些无线系统的基本测试证实了引起 WSN 产生互扰的原因。互扰抑制策略通常包括受扰系统和互扰源的物理分离和频段分离、有效路由协议的使用及运用频率自适应等。本章研究了 WSN 运行中的无线互扰的定义、成因及有效抑制方案。

7.2　无线传感器网络的共存与互扰

共存是指某一系统与其他可能使用或不使用相同规范的系统共享特定环境的情况下执行任务的能力（IEEE，2000）。例如，对一个家庭部署一个基于 ZigBee 的智能家居系统，一个主要部署问题就是确保 ZigBee 系统和家居 Wi-Fi 系统共存。对森林火灾监测、环境和交通监控等大规模 WSN 部署问题，WSN 与其他无线系统的共存就是确保 WSN 具有令人满意的性能。

无线通信中互扰的概念通常是指下面两个概念之一：（1）多个（即多于两个）数据包同时传输时在接收端发生的碰撞；（2）无线传播信道的物理因素（Golmie，2006）。

如果多个无线信号同时到达接收端，接收端将不能提取任何有用的信息，因为期望信号和互扰信号互相重叠。

无线传播信道的物理因素是互扰无线通信系统正常运行的另一个问题。因此，设计无线系统时应考虑各种物理互扰，如多径传播。多径传播是指传输信号可以沿着不同的路径（如房屋、窗户或墙壁的反射）到达接收端。图 7.1 给出了多径传播的实例。

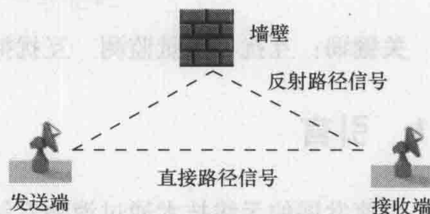


图 7.1 多径传播的实例

如图 7.1 所示，介于发送端和接收端之间的信号的直接路径为期望无线信号路径，也称作视距（Line of Sight，LoS）连接。如果障碍物（如图 7.1 所示的墙壁）位于发送端附近，无线信号可能被反射，并沿着反射路径到达接收端。功能简单的接收端不能区分多径信号，它只是把这些信号加起来，因此直接路径信号和反射路径信号就会发生互扰（Molisch，2005）。

本章关于互扰的研究主要是讨论和测评由其他无线系统，特别是 IEEE 802.11b Wi-Fi 系统对 IEEE 802.15.4 WSN 造成的影响，并重点关注了数据包连续传输的问题。

7.3 性能指标

在 IEEE 802.15.4 WSN 中，评价无线通信的性能指标可以分为两类：PHY 层和 MAC 层指标。这些指标通常用于衡量干扰的程度。

7.3.1 物理层性能指标

SNR 是无线系统物理层常用的性能指标，它表示平均信号功率和平均噪声功率之比，单位为 dB。无线系统必须在某一频率上发送调制信号。接收端只能在同一频率上保持侦听才能使调制信号接收成功。如果 SNR 小于预定义的阈值，这意味着噪声值大于期望信号值，那么接收端将不能获得期望信号（Chandra 等，2007）。另一个重要的性能指标为 BER，其含义是在数据传输中接收端接收到的错误比特数与传输总比特数的百分比。某些无线系统因为使用的调制方案不一样，所以对满足可接受性能指标的 SNR 和 BER 的要求也不一样。图 7.2 给出了两种无线标准的 SNR-BER 的仿真结果。

图 7.2 所示的仿真结果是多个无线技术在不同的 SNR 下的仿真结果。总的趋

势是随着 SNR 的增加 BER 降低。例如，如果 IEEE 802.15.4 的系统要求达到 1.0×10^{-9}的 BER，那么相应的 SNR 就应大于 3dB。换句话说，一旦噪声大到一定的值，能正确恢复的比特数就相应地降低。当 IEEE 802.15.4 信号被 IEEE 802.11b（即 Wi-Fi）强信号互扰时，这种情况通常会发生。

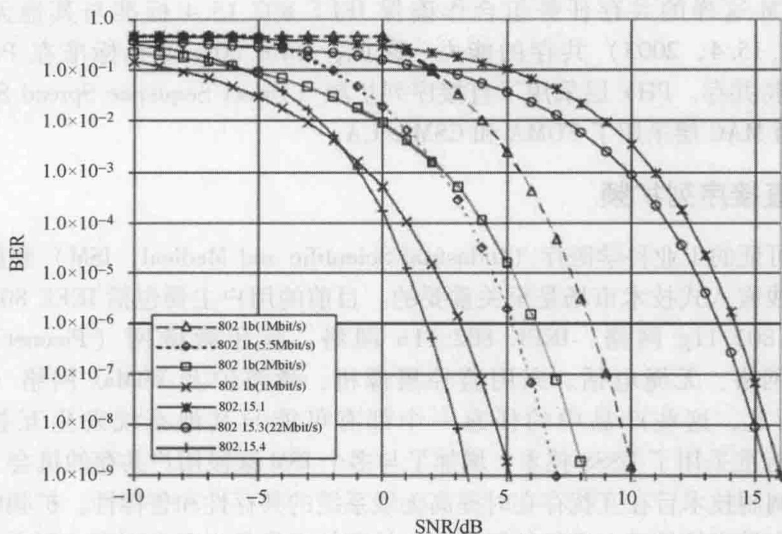


图 7.2　IEEE 802.11b 与 IEEE 802.15（IEEE 802.15.4，2003 年）的 BER-SNR 的仿真结果

7.3.2　媒体访问控制层性能指标

对开发人员来说，理解 SNR 和 BER 这样的无线通信物理层性能指标虽然重要，但是当系统被互扰时，如果没有特定的设备很难得到这些性能指标的测量值。最常用的测评是直接测试。例如，误包率（Packet Error Rate，PER）用来描述特定环境下无线系统的可持续性，在 MAC 层可以实现 PER 的测量。

MAC 层是由协调信道访问和共享机制的规则构成的，通常负责经过 PHY 层的数据包的组装和分解。为了在系统级层面上分析互扰对 WSN 的影响，性能指标应包括 PER、传输延迟和吞吐量（Shin 等，2007）。

PER：PER 是指数据包丢失的百分比，可以表达为接收端未接收的数据包与发送端发送的所有数据包的比（Cuomo 等，2007）。在 WSN 中，由互扰引起的一个结果就是导致误包率变大。误包率也是最重要的性能指标之一，它可以通过互扰抑制设计得到改善。

延迟和吞吐量：吞吐量是指在一定的时间段内从一个站到另一个站传送的数据量（Shin 等，2007）。在 WSN 中，互扰的发生会明显地使传输延迟增加吞吐量降低，这两个指标可以在系统级层面上通过有效的互扰抑制设计得到改善。

7.4 IEEE 802.15.4 中的共存机制

在设计 IEEE 802.15.4 标准的过程中，IEEE 802.15.4 任务组与其他如 IEEE 802.15.2TM 这样的共存任务组合作确保 IEEE 802.15.4 标准与其他无线设备（IEEE 802.15.4，2003）共存的能力。因此，IEEE 802.15.4 标准在 PHY 层和 MAC 层支持共存。PHY 层采用了直接序列扩频（Direct Sequence Spread Spectrum，DSSS），而 MAC 层采用了 FDMA 和 CSMA/CA。

7.4.1 直接序列扩频

免许可证的工业科学医疗（Industrial Scientific and Medical，ISM）频段对蓬勃发展的无线嵌入式技术市场是至关重要的。目前的用户主要包括 IEEE 802.11b 网络、IEEE 802.11g 网络、IEEE 802.11n 网络、蓝牙微微网（Piconet）、IEEE 802.15.4 网络、无绳电话、家用监控摄像机、微波炉及 WiMax 网络（ZigBee，2007）。因此，这些产品中的任意一个都有可能与其他系统发生互扰。IEEE 802.15.4 标准采用了 DSSS 技术，增加了与多个 ISM 频段用户共存的机会。

扩频调制技术旨在互扰存在时提高无线系统的共存性和鲁棒性。扩频的概念就是在一个高带宽的信道上进行扩展传输。扩频技术最早出现在军事应用中。之所以使用扩频技术是因为它具有一些吸引力的特性，如抗干扰性能、低概率截获和多路访问通信（Fakatselis，1996）。一般情况下，即使窄带信号（编码和信息传输使用小带宽的信号）的中心频率不完全相同，信号冲突和数据包丢失仍然可能发生。虽然频率分配受到如美国联邦通信委员会这样的管理者的约束和控制，但是对 ISM 频段却没有强制性要求。因此任何使用窄带信号（IEEE 802.15.4，2003）的无线系统都可能发生无线互扰。图 7.3 所示为两个窄带信号发生冲突的例子。

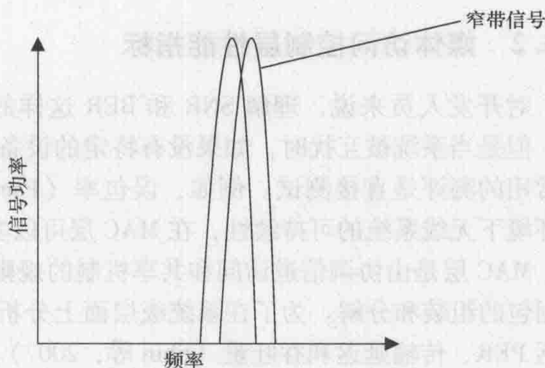


图 7.3　两个窄带信号发生冲突的例子（ZigBee，2007）

由于这两个信号的主体部分互相重叠，所以重叠部分携带的信息由于互扰就会受到破坏。为避免窄带信号之间无法控制的互扰，应对重叠部分的有效区域进行限制。扩频方法就是为解决这个问题而设计的。图 7.4 给出了扩频原理。

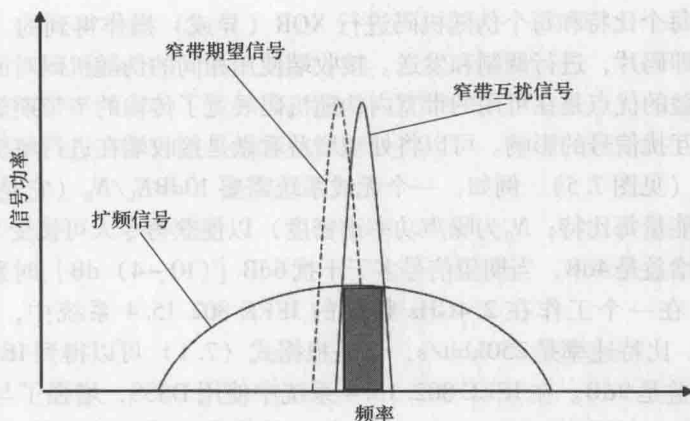


图 7.4　扩频原理

如图 7.4 所示，两个窄带信号分别表示窄带互扰信号（实线）和窄带期望信号（虚线）。扩频的目的就是用较宽的带宽去传输窄带期望信号所携带的原始比特信息。经过扩频，只有一小部分原始窄带期望信号受到窄带互扰信号的影响（图 7.4 所示灰色方块部分）。当扩频信号到达接收端时，系统会从扩频信号中提取出有用信号。

如图 7.5 所示，扩频信号经过接收端滤波器恢复为未扩信号的形式。接收端滤波器的主要作用是使接收端只对指定频率的信号敏感。尽管一部分窄带互扰信号也会通过接收端滤波器，但是非常有可能获得正确的期望窄带信号，因为只有一小部分扩频信号受到互扰的影响。从理论上说，传输扩频信号的带宽越宽，就越能抑制互扰。处理增益 G 是扩频技术中的一个常用指标（Golmie，2006）：

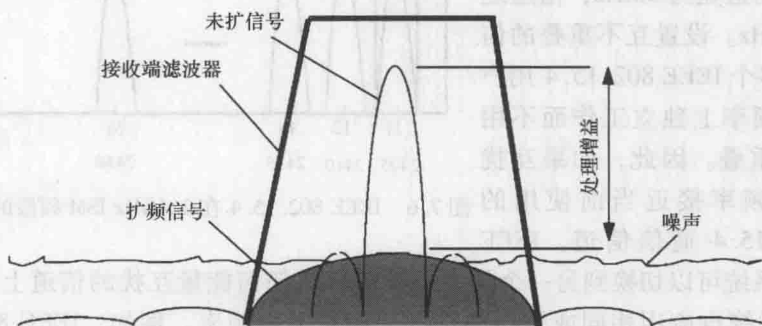


图 7.5　接收端的 DSSS（Fakatselis，1998）

$$G = 10\log_{10}(r_c/r_b) \tag{7.1}$$

式中，r_b和 r_c分别为比特率和码片率。在 DSSS 系统中，每个比特在传输前被分解成称为码片的比特串模式。

码片是对每个比特和每个伪随机码进行 XOR（异或）操作得到的。然后对异或操作的结果，即码片，进行调制和发送。接收端使用相同的伪随机码对原始数据进行解码。处理增益的优点是在可用的带宽内伪随机码展宽了传输的窄带期望信号，使它较少受到窄带互扰信号的影响。可以将处理增益看做是接收端在进行解扩操作之后信号与互扰之比（见图7.5）。例如，一个无线系统需要 10dBE_b/N_0（它是 SNR 的归一化形式；E_b为能量每比特；N_0为噪声功率谱密度）以便获得令人可接受 BER 的性能。如果系统处理增益是4dB，当期望信号多于干扰6dB［（10－4）dB］时系统能维持所要求的性能。在一个工作在 2.4GHz 频段的 IEEE 802.15.4 系统中，码片速率是2000kchip/s[⊖]，比特速率是250kbit/s，于是根据式（7.1）可以得到IEEE 802.15.4设备的处理增益是9dB。在 IEEE 802.15.4 系统中使用DSSS，增强了与信号带宽小于 IEEE 802.15.4（IEEE 802.15.4，2003 年）的窄带无线通信系统（如蓝牙）有效共存的能力。

尽管无线系统的设计有助于 IEEE 802.15.4 的设备在一定程度上（如互扰功率小于期望信号功率时）改善互扰抑制的性能，但是不可能克服所有的互扰，特别是当干扰信号远强于期望信号时。

7.4.2　频分多址

IEEE 的 802.15.4 系统所使用 FDMA 将 2.4GHz ISM 频段划分成16 个互不重叠的信道，如图 7.6 所示。

如图 7.6 所示，2.4GHz 频段从 2405MHz 开始到 2480MHz 结束共定义了 16 个信道。每个 IEEE 802.15.4 信道宽为 2MHz，信道之间相距 5MHz。设置互不重叠的信道可以使多个 IEEE 802.15.4 用户在不同的频率上独立工作而不用担心互相重叠。因此，如果互扰无线信号频率接近当前使用的 IEEE 802.15.4 通信信道，IEEE 802.15.4 系统可以切换到另一个其中心频率远离任何能量互扰的信道上。其他的一些无线系统也应用相同或类似的机制来使用无线频率。例如，IEEE 802.11b/g 技术使用相同的 FDMA 机制在 2.4GHz 频段上定义了 14 个通信信道。蓝牙技术（即 IEEE 802.15.1）将科学频段（S-Band）划分成 79 个带宽为 1MHz 的信道，并

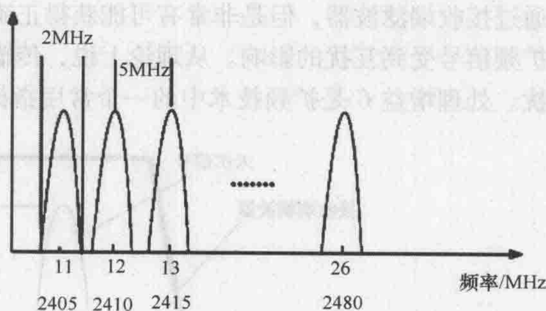


图 7.6　IEEE 802.15.4 在 2.4GHz ISM 频段的信道分配

⊖ chip：码片。

使用跳频（Frequency Hopping，FH）实现无线通信。此系统在定义好的信道中不断地跳频。发送端使用的信道顺序或者说跳频序列是预定义的，并提前发送给接收端。发送端在每个信道上使用的时间应小于 400ms，最大功率应不超过 1W。由于跳频，蓝牙设备通过定期切换信道的方式能很容易地避免互扰的影响。

7. 4. 3　具有冲突避免的载波侦听多路访问

由于 IEEE 802. 15. 4 设备可能与不同的无线系统共存，IEEE 802. 15. 4 MAC 协议采用 CSMA/CA 技术来处理不可预测的互扰或 IEEE 802. 15. 4 设备进行通信时信号发生冲突的情况。CSMA/CA 技术广泛应用于其他通信网络，如以太网和 Wi-Fi。该技术使用了简单的“先听后说”策略。在进行无线传输之前，设备在信道上进行侦听并完成信道评估。如果信道空闲，则开始发送。如果信道忙，则设备在等待一个随机时间之后继续进行信道评估。随着信道评估失败次数的增加，等待时间将按指数增长以避免冲突（ZigBee，2007）。

上面提及的所有机制对保证基于 IEEE 802. 15. 4 的 WSN 的共存非常有用，然而它们只在不同的情况下才起作用。DSSS 技术有助于无线传输提高接收端成功接收的可能性，FDMA 通过搬移不同的无线频率信道为 IEEE 802. 15. 4 系统提供了较大的和其他无线系统共存的机会，CSMA/CA 的目的是在真正传播无线信号之前处理信号冲突。当 WSN 应用于实际应用时，可能发生由不同应用引起的各种情况，因此在设计互扰抑制策略时需要充分考虑到这一点。

7. 5　IEEE 802. 11b 和 IEEE 802. 15. 4 间的互扰抑制

现有的研究表明只有当下面的两个条件满足时互扰才能发生：无线频段分离很小或为零；能量干扰很大。这里的频段分离是指两个相关通信信道的中心频率的差值。

7. 5. 1　频段分离

IEEE 802. 15. 4 和 IEEE 802. 11b 设备都工作在指定的通信信道。由于 2. 4GHz ISM 频段范围有限，两个无线系统很有可能在相近的频率上工作。无线发送功率通常集中在指定信道的中心频率附近，因此如果频段分离很小就很容易产生互扰。IEEE 802. 15. 4 和 IEEE 802. 11b 在 2. 4GHz ISM 频段的信道分配如图 7. 7 和表 7. 1 所示。IEEE 802. 11b 有 14 信道，信道中心频率范围为 2412 ~ 2473MHz，信道带宽为 22MHz，相邻信道间隔为 5MHz。由于 IEEE 802. 11b 信道带宽宽，许多通信信道互相重叠。为保证多个 IEEE 802. 11b 网络能同时在相近区域工作，任意 IEEE 802. 11b 通信信道之间的频率间隔必须至少为 30MHz（So，2004）。因此 IEEE 802. 11 标准建议，如果多个 IEEE 802. 11b 网络需要在同一区域工作，可以使用 3

个非重叠的信道。如图 7.7 所示，不同的地域对这三个互不重叠的信道设置不一样：在中国和北美推荐信道 1、6 和 11 而在欧洲则选用 1、7 和 13（IEEE 802.11，2007）。

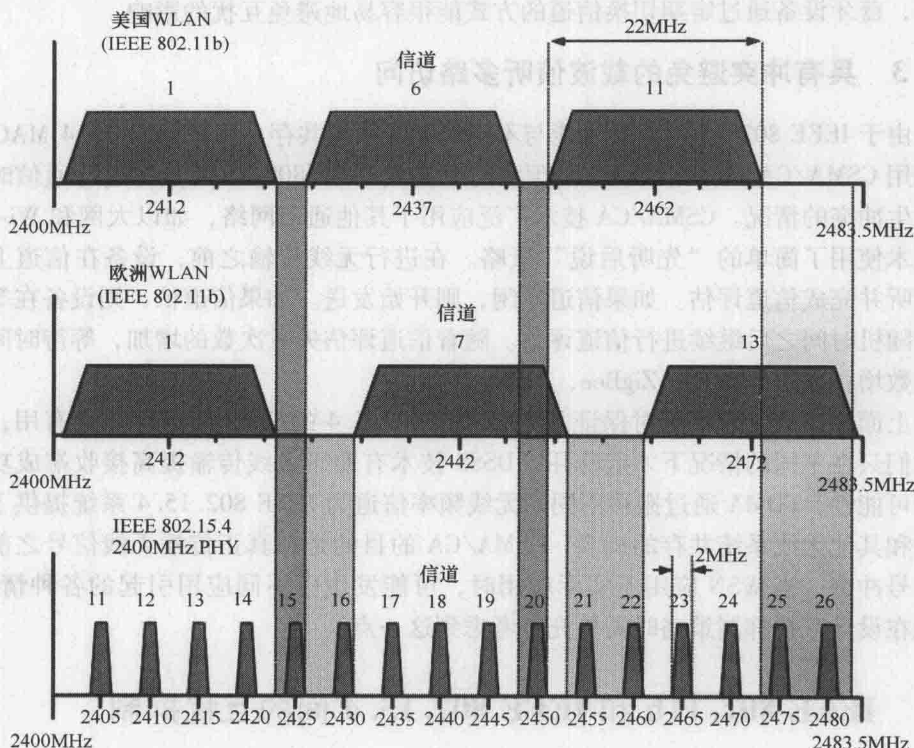


图 7.7　IEEE 802.11b 和 IEEE 802.15.4 在 2.4GHz ISM 频段的信道分配

另一方面，IEEE 802.15.4 在 2.4GHz 频段共有 16 个信道，信道间隔为 5MHz，信道带宽为 2MHz。IEEE 802.15.4 的信道号从 11 开始，因为 IEEE 802.11b 的 PHY 层在 868MHz 频段占据 1 个信道，在 915MHz 频段占据 10 个信道。每个 IEEE 802.11b 信道的频段与 4 个 IEEE 802.15.4 信道的不同频段重叠。例如，IEEE 802.11b 信道 1 的频段为 2401 ~ 2423MHz，包括了 IEEE 802.15.4 信道 11 ~ 14 的频段。IEEE 802.11b 的信道 1 在 IEEE 802.15.4 的信道 11 ~ 14 附近工作时能导致无线互扰。

如图 7.7 所示，除了深灰色所示的一些信道外，IEEE 802.15.4 的大部分通信信道与 Wi-Fi 通信信道重叠。这些信道提供了一种简单的共存方式。例如，IEEE 802.15.4 的信道 15、20、25 和 26 所用的频段位于 IEEE 802.11b 信道 1、6 和 11 所用的频段之外。因此，IEEE 802.15.4 的那些信道可以应用于某些已经考虑了来自 IEEE 802.11b 互扰的环境。但是，还存在许多必须使用更多 IEEE 802.15.4 信

道的情况，这些信道就有可能遭受互扰。

即使 IEEE 802.11b 和 IEEE 802.15.4 都使用了 DSSS 技术，如果 IEEE 802.11b 和 IEEE 802.15.4 系统的中心频率很接近，扩频的优势也不会产生任何明显的效果。另外，IEEE 802.11b 设备的最大传输功率可以达到 20dBm（相当于 100mW），远大于 IEEE 802.15.4 设备（即 1mW）。一旦 IEEE 802.11b 信号影响了 IEEE 802.15.4 设备的接收，相对较高的输出功率将会导致 SNR 的噪声增加。图 7.8 给出了IEEE 802.11b 的传输频谱模板。

表 7.1　IEEE 802.15.4 和 IEEE 802.11b 在 2.4GHz ISM 频段的信道分配

IEEE 802.11b		IEEE 802.15.4	
信　道	频率/GHz	信　道	频率/GHz
1	2.401 ~ 2.423	11	2.405
2	2.406 ~ 2.428	12	2.410
3	2.411 ~ 2.433	13	2.415
4	2.416 ~ 2.438	14	2.420
5	2.421 ~ 2.443	15	2.425
6	2.426 ~ 2.448	16	2.430
7	2.431 ~ 2.453	17	2.435
8	2.436 ~ 2.458	18	2.440
9	2.441 ~ 2.463	19	2.445
10	2.446 ~ 2.468	20	2.450
11	2.451 ~ 2.473	21	2.455
12	2.456 ~ 2.478	22	2.460
13	2.461 ~ 2.483	23	2.465
14	2.466 ~ 2.488	24	2.470
		25	2.475
		26	2.480

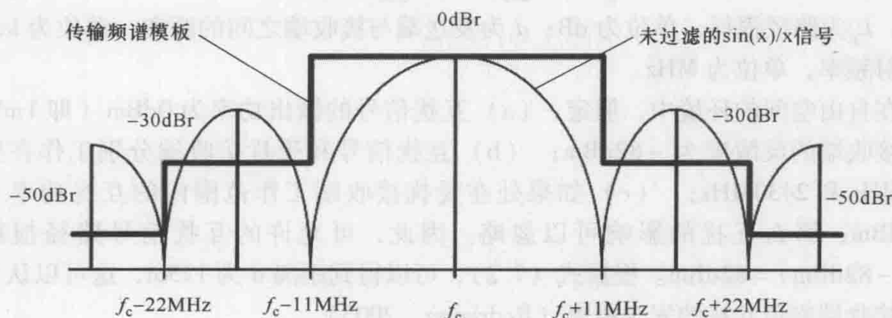


图 7.8　IEEE 802.11b（IEEE 802.11，2007）的传输频谱模板

如图 7.8 所示，功率谱集中在选定的 IEEE 802.11b 通信信道的中心频率上。与中心频率距离越远，IEEE 802.11b 的信号功率就越低。Shin 等人的参考文献（2007）对互扰与频段分离之间的关系进行了仿真研究。仿真结果表明，当这两个系统的中心频率的频段分离大于 7MHz，IEEE 802.15.4 系统可以达到令人接受的性能（即 PER 小于 1%）。Petrova 等人的参考文献（2006）也进行了类似的研究。对 IEEE 802.15.4 和 IEEE 802.11b 通信信道之间的中心频率的频段分离进行了不同的测评。可以得到下面的结论：测评结果显示，为了获得令人满意的性能，IEEE 802.15.4 工作频率之间的频段分离至少应为 7MHz。

7.5.2 能量互扰和物理分离

能量互扰是引起无线接收节点接收故障的主要原因。正如前面提到的，除非能量干扰强度小于可接受的值，否则较强的能量干扰容易使接收节点无法识别期望信号。

无线通信互扰起作用的有效范围主要由互扰发送端到受扰接收端的物理距离决定的。衡量无线系统性能通常有两个参数：输出功率和接收端灵敏度。

- 输出功率，表明发送端发出的输出信号的能量强度。
- 接收端灵敏度，表示无线信号的最小能量强度，可以在接收端检测到。

如果到达接收端的输出信号的剩余能量大于接收端灵敏度，那么接收端就能够恢复无线信号。经过传播，输出信号的能量会随着信号传播距离的增加而衰减。当互扰发送端和受扰接收端相隔一定的物理距离时，到达受扰接收端的互扰信号强度将会减弱。如果互扰信号的剩余信号强度小于允许的噪声强度，那么受扰接收端就能够正常工作。信号强度的减弱属于路径损耗。路径损耗指的是发送端天线的总发送功率乘以接收端的天线接收方向数值增益与接收端天线的可用功率的比值（Chandra 等，2007）。根据不同的环境条件，路径损耗可以描述为不同的模型。其中基本模型就是路径损耗应用到最简单的环境的情况：自由空间中只有发送端和接收端。模型（Yilmaz，2002）可表示为

$$L_p = 20\log_{10}d + 20\log_{10}f + 32.45 \tag{7.2}$$

式中，L_p为路径损耗，单位为 dB；d 为发送端与接收端之间的距离，单位为 km；f 为发射频率，单位为 MHz。

在自由空间的环境中，假定：（a）互扰信号的输出功率为 0dBm（即 1mW），受扰接收端的灵敏度为 -82dBm；（b）互扰信号和受扰接收端分别工作在频率 2410MHz 和 2430MHz；（c）如果处在受扰接收端工作范围内的互扰功率小于 -82dBm，那么互扰的影响可以忽略。因此，可允许的互扰信号路径损耗为 0-(-82dBm)=82dBm。根据式（7.2），可以得到距离 d 为 125m，这可以认为是受扰接收端避免互扰的安全距离（Rodriguez，2005）。

在实际环境中，路径损耗的计算受到许多因素的影响，如天线、建筑结构和街道布局等。Shin 等人的参考文献（2007）使用下面的简单室内路径损耗模型分析

了由 IEEE 802.11b 发送端引起的 IEEE 802.15.4 系统的互扰：

$$L_{\mathrm{p}}(d)=\begin{cases}20\log_{10}\left(\dfrac{4\pi d}{\lambda}\right) & d\leqslant d_0\\ 20\log_{10}\left(\dfrac{4\pi d}{\lambda}\right)+10n\log_{10}\left(\dfrac{d}{d_0}\right) & d>d_0\end{cases} \tag{7.3}$$

式中，d 为发送端和接收端之间的距离，单位为 m；d_0为视距，单位为 m，通常为 8m；$\lambda=c/f_c$，c 为光速，f_c为载波频率（MHz）；n 为路径损耗指数，其值在距离超过 8m 的室内环境下为 3.4（Golmie 等，2005）。对于 IEEE 802.15.4 和 IEEE 802.11b 系统来说，在输出功率确定的情况下，可以得到下面的接收端的接收功率（Shin 等，2007）：

$$P_{\mathrm{R}}=P_{\mathrm{T}}10^{\frac{-L_{\mathrm{p}}(d)}{10}} \tag{7.4}$$

式中，P_{T}为在发送端测量得到的发送功率，单位为 mW；P_{R}为在接收端测量得到的接收功率，单位为 mW；$L_{\mathrm{p}}(d)$ 为发送功率经过距离 d 之后的路径损耗，单位为 dB。

式（7.4）也表明，发送功率随着通信距离的增加而减弱。期望信号（IEEE 802.15.4）和互扰（IEEE 802.11b）这两者的接收功率可以通过改变 IEEE 802.15.4 接收端和 IEEE 802.11b 发送端之间的物理间隔进行调整。一方面，如果这两者之间的物理距离足够大，那么 IEEE 802.11b 的发送功率不会影响到 IEEE 802.15.4 接收端。另一方面，如果 IEEE 802.15.4 信号（期望信号）的接收功率大于接收端灵敏度且接收端的信干噪比（Signal to Interference and Noise Ratio，SINR）大于其阈值，那么 IEEE 802.15.4 接收端和 IEEE 802.11b 发送端之间的物理分离为距离 d 是安全的，否则在部署方面则需要一个更远的物理分离。SINR 是 SNR 的扩展，可以由下式确定：

$$\mathrm{SINR}=10\log_{10}\left(\frac{P_{\mathrm{R}}^{\mathrm{s}}}{P_{\mathrm{R}}^{\mathrm{i}}+P_{\mathrm{R}}^{\mathrm{n}}}\right) \tag{7.5}$$

式中，$P_{\mathrm{R}}^{\mathrm{s}}$、$P_{\mathrm{R}}^{\mathrm{i}}$和 $P_{\mathrm{R}}^{\mathrm{n}}$分别为接收端的期望信号功率、互扰功率和噪声功率。

Shin 等人的参考文献（2007）在仿真中假定 IEEE 802.11b（互扰系统）和 IEEE 802.15.4（受扰系统）的输出功率分别为 30mW 和 1mW。IEEE 802.11b 系统发送速率为 11Mbit/s，载荷为 1500 字节；IEEE 802.15.4 发送速率为 250kbit/s，载荷为 105 字节；IEEE 802.11b 系统和 IEEE 802.15.4 系统之间的中心频率的频段分离为 2MHz。此外，假设 IEEE 802.11b 信号为非均匀功率谱密度分布。仿真结果显示，当 IEEE 802.15.4 接收端和 IEEE 802.11b 发送端之间的距离大于 8m 时，IEEE 802.15.4 系统的 PER 小于 10^{-5}。

7.5.3　IEEE 802.15.4 中的互扰抑制建议

IEEE 802.15.4 任务组已经为免许可证频段的 IEEE 802.15.4 系统与其他无线

设备的共存制定了一个通用准则。IEEE 802.15.4 标准中的共存机制包括空闲信道评估（Clear Channel Assessment，CCA），动态信道选择，调制、能量检测（Energy Detection，ED）和链路质量指示（Link Quality Indication，LQI），低占空比，低发送功率，以及信道调整（IEEE 802.15.4，2003）。

- CCA。CCA 是 CSMA/CA 机制中的一部分。可以使用的 CCA 方法有三种：过阈值能量检测，具有 IEEE 802.15.4 特征的信号检测，或者这两种方法的组合。IEEE 802.15.4 的 PHY 层可以选择一种 CCA 方法实现信道评估以检测是否有其他设备占用信道。

- 动态信道选择。IEEE 802.15.4 标准不支持直接跳频。但是，如果当前的信道检测到互扰时，用户可以在应用中指定一种机制手动切换到一个合适的通信信道。

- 调制、ED 和 LQI。IEEE 802.15.4 标准所使用的调制方法为偏移正交相移键控（Offset Quadrature Phase Shift Keying，O-QPSK），它是一种可以获得低 SNR 和低功耗的调制方法。ED 和 LQI 是两个测量函数。ED 用来检测 IEEE 802.15.4 信道的能量强度，并为高层的信道选择算法提供有用信息。LQI 用来测量接收的数据包的信号强度，通常用作信号质量的指示。

- 低占空比。这是一种对工作方式的要求。对用于环境监测的 WSN 来说，单个 IEEE 802.15.4 设备发送传感器读数（如 1 字节的温度读数）报告的时间间隔为 1min 或以上是合理的。例如，如果 IEEE 802.15.4 数据包载荷为 22 字节，每分钟发送 250kbit/s 的数据，那么所需发送时间为 $22\times8\text{bit}/250\text{kbit/s}=0.704\text{ms}$。因此，IEEE 802.15.4 设备的占空比为 $0.704/(1\times60\times1000)=1.17\times10^{-3}\%$，发送端在剩余的工作周期内处于不活动状态。采取低占空比的工作方式明显地减小了互扰信号与 IEEE 802.15.4 设备竞争的可能性。

- 低发送功率和信道调整。低发送功率是一种主要用于提高 IEEE 802.15.4 设备与其他无线系统共存的能力。虽然美国联邦通信委员会（Federal Communication Commission，FCC）的标准允许 2.4GHz 频段的发送功率最大为 1W，但是 IEEE 802.15.4 设备允许以较小的发送功率（即典型的为 1mW）工作来尽量减少与其他无线设备的互扰。信道调整要求 IEEE 802.15.4 和潜在的无线系统之间的通信信道有一个恰当的分离，这能够使多个无线系统同时工作而没有明显的互扰。

7.6 先进互扰抑制策略

人们对互扰抑制正在开展广泛的研究。信道切换和连续数据传输是其中的两个热点。当互扰发生时，将基于 IEEE 802.15.4 的 WSN 的当前工作信道切换到相对空闲的频率上是一种比较容易和有效的互扰抑制方式。另外，在一定时间内进行连续数据传输可避免额外的信道切换代价。本节将回顾现有典型的互扰抑制策略。

7.6.1　自适应互扰感知的多信道分簇

Kang 等人的参考文献（2007）提出了一种自适应互扰感知多信道分簇算法来避免 ZigBee 网络的 IEEE 802.11 互扰。该算法假设 ZigBee 网络是静态的，即不允许改变拓扑和增加节点。分簇 ZigBee 网络典型拓扑如图 7.9 所示。

图 7.9 所示的拓扑对 ZigBee 设备进行了分簇。除了 PAN 调节器，每个簇都有一个负责簇和 ZigBee 设备管理的簇头。每个簇都有一个用来建立通信的 CID。有两种使用信道的方式：簇内设备使用的簇内信道，以及簇头和桥设备（Bridge Device，BRD）使用的簇间信道。BRD 是直接连接邻簇簇头的节点。使用簇间是为了增加 ZigBee 网络的覆盖范围。算法由下面两步组成：

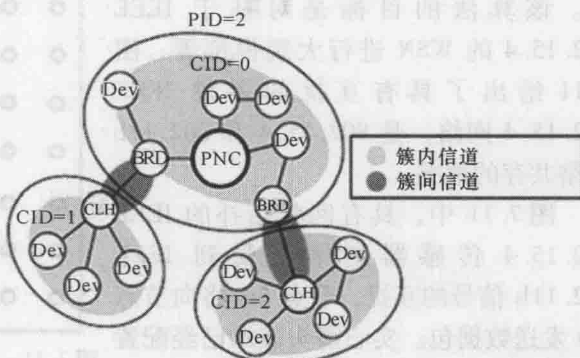


图 7.9　分簇 ZigBee 网络典型拓扑（Kang 等，2007）

- 互扰监测。一旦簇内设备检测到 IEEE 802.11 互扰的存在（如同步信标或确认帧的丢失），则向本簇广播一个信道变化广播报文（Channel Change Broadcast Message，CCBM），以让簇内其他设备都检测到互扰。
- 互扰避免。簇内设备一旦收到 CCBM，就将信道切换到一个新的信道。为确保每个设备都切换到同一个信道而不增加额外的开销，可以将 PAN 标识、CID、当前信道和信道切换计数器的组合作为产生下一信道的索引。具有相同参数的设备可以获得相同的结果，如图 7.10 所示，这些参数作为伪随机序列发生器（Pseudo Random Sequency Generator，PRSG）的输入。

对于簇间连接，簇头周期性地向桥节点发送一个测试帧。如果一些确认帧丢失，簇头就假定簇间信道存在互扰，它发送一个 CCBM 帧，并切换到一个新的信道上。对于桥节点，如果一些测试帧没有按期接收，则向它所在的簇也发送一个 CCBM 帧，然后切换到一个新的信道上。

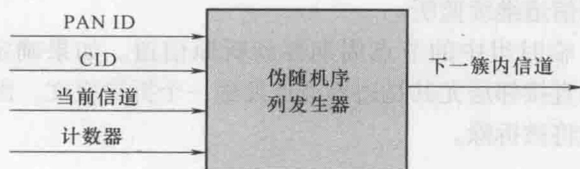


图 7.10　伪随机序列发生器框图

7.6.2 自适应无线信道分配

Won 等人的参考文献（2005）提出了一种支持 IEEE 802.15.4 和 IEEE 802.11b 共存的自适应无线信道分配算法。该算法的目标是对基于 IEEE 802.15.4 的 WSN 进行大规模部署。图 7.11 给出了具有互扰的多跳 IEEE 802.15.4 网络，是 802.15.4 和 802.11b 网络共存的情况。

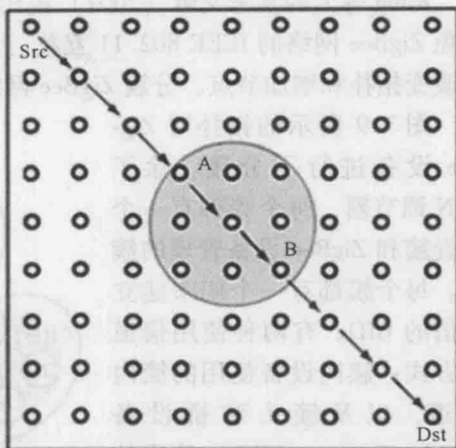


图 7.11　具有互扰的多跳 IEEE 802.15.4 网络

图 7.11 中，具有网状拓扑的 IEEE 802.15.4 传感器网络正受到 IEEE 802.11b 信号的互扰，节点 Src 将向节点 Dst 发送数据包。实心箭头表示已经配置好的从源节点到目的节点的路由。阴影区域是受到互扰影响的部分网络。如果源节点能重新选择一条新路由绕过受扰区域，就可以解决互扰问题。但是，会导致额外的计算开销。Won 等人的参考文献（2005）提出了一种使互扰区域内节点临时切换通信信道的方式来降低额外路由选择开销的策略。策略的实现由三个步骤组成：互扰监测、组的建立与拆除。

● 互扰监测。IEEE 802.15.4 网状网络内的每个节点使用标准的能量检测或信道空闲评估功能来检测数据的吞吐量和执行互扰侦测。一旦检测到吞吐量突然下降，且能量检测返回一个较大的值，节点就进入组建立过程以在一个空闲信道内建立一个临时组。

● 组的建立。发起组建立过程的节点应向其直接邻居节点提供准备切换的信道报文。邻居节点一收到这个报文就更改其原来的角色去担当边界节点，从而在原网络和互扰区域内的节点之间建立起一个桥。边界节点通过新信道向发起组建立的节点发送一个回复报文。回复报文就是确认边界节点已注意到情况发生了变化。然后，边界节点切换回原信道。如果边界节点为加入临时组的节点接收新到的数据，则立即切换到临时组使用的信道，并向期望节点发送数据。边界节点在数据发送完成之后就返回到原信道继续监听。

● 组的拆除。临时组中的节点周期性侦听原信道。如果确定信道是空闲的，则节点就向所有的直接邻居尤其是边界节点发送一个拆除报文。因此，当互扰完全消失时，整个组就将被拆除。

7.6.3 连续数据传输

如果 IEEE 802.15.4 系统受到互扰，可以使用连续数据传输这个干扰抑制策略

维持通信（Yao 和 Yang，2010）。假设 IEEE 802.15.4 设备受到互扰时通信成功率为 $R_{\text{Interference}}$，且系统在连续发送 n 个数据包之后至少成功通信一次的概率为 P_{Success}，那么有下式成立：

$$1-(1-R_{\text{Interference}})^{n} \geqslant P_{\text{Success}} \tag{7.6}$$

且连续传输数据包数 n 为

$$n \geqslant \frac{\log_{10}(1-P_{\text{Success}})}{\log_{10}(1-R_{\text{Interference}})} \tag{7.7}$$

如果给定可以从基准测试中得到的通信成功率 $R_{\text{Interference}}$，由式（7.7）就可以得到保证通信成功的连续发送数据包数。例如，如果选定 $R_{\text{Interference}}$ 为 25%，达到符合要求的概率 P_{Success} 为 90%，那么 IEEE 802.15.4 设备应发送 8 次（即 $n=8$）数据请求包。如果在连续数据传输之后没有收到期望的确认，就可以认为 IEEE 802.15.4 受到了严重的互扰。然后，IEEE 802.15.4 就启动能量检测，并切换到一个具有最小能量活动的空闲信道上。

7.6.4　多跳数据传输控制

IEEE 802.15.4 移动自组网需要多跳数据传输时，尤其是进行大量数据传送时，传输时间间隔的设定是确保传输成功的关键。与一对设备完成数据传输过程相比，多跳数据传输具有较高的传输失败率，因为其中一段通信链路故障就可以中断整个通信过程。

7.6.4.1　两个连续传输数据包之间的传输时间间隔

图 7.12 给出了多跳传输的简化模型。图 7.12 中，多跳传输模型可以描述为一个传输链；设备 A 为源设备；设备 D 为准备接收设备 A 数据的目的设备。多跳数据传输的性能可以用到达率（Arrival Rate，AR）来测量。AR 表示的是成功到达目的设备的数据与源设备发送的全部数据之比。

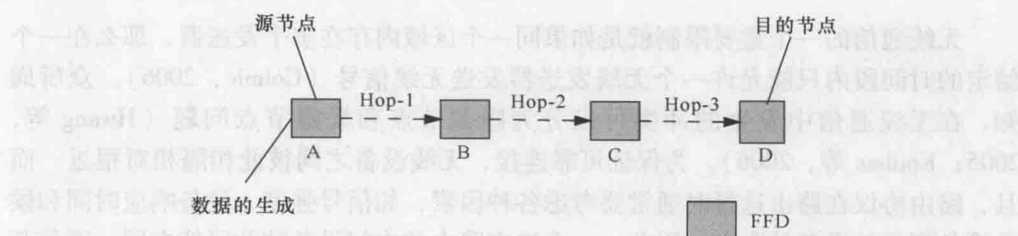


图 7.12　多跳传输的简化模型

根据 IEEE 802.15.4 标准，设备 A 应完成以下三个标准步骤以确保数据传输成功：

- 实现 CSMA/CA 来检测信道是否空闲以进行数据传输；
- 向下一跳发送数据；

● 等待来自下一跳的确认。

路由上的中间设备 B 和设备 C 需要以下四个步骤来完成中继任务：

● 接收路由上的前驱节点发送的数据，然后按需回送确认；
● 实现 CSMA/CA 来检测信道是否空闲以进行数据传输；
● 向下一跳发送数据；
● 等待来自下一跳的确认。

多跳传输的目的设备 D 需要接收设备 C 转发的数据，并按需回送确认。图 7.13 所示为基于相同时间线的多跳数据传输。

图 7.13 中，对同一时间线上设备在多跳数据传输中采取的动作进行了比较。从理论上讲，如果数据经设备 B 成功地转发到设备 C，源设备 A 就可以为后面的数据包进行新的数据传输。但是，如果数据传输没有调度好或者传输的时间间隔太小，就会发生数据包冲突。

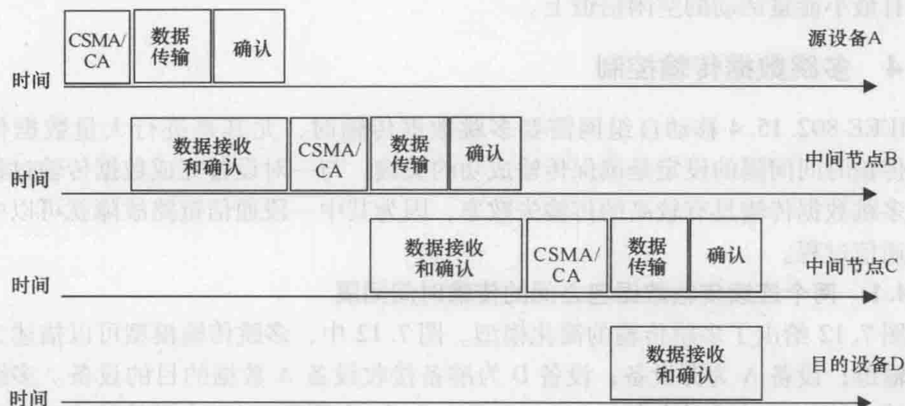


图 7.13　基于相同时间线的多跳传输

无线通信的一个重要限制就是如果同一个区域内存在多个发送器，那么在一个给定的时间段内只能允许一个无线发送器发送无线信号（Golmie，2006）。众所周知，在无线通信中发生的冲突可以分为隐藏节点和暴露节点问题（Hwang 等，2005；Koubaa 等，2006）。为保证可靠连接，无线设备之间彼此相隔相对很近。而且，路由协议在路由选择时通常要考虑各种因素，如信号强度、设备响应时间和候选设备到目的设备的距离。因此，一个选定路由的中间设备彼此可能在同一通信范围内。对图 7.12 所示的简化模型，假定设备 A 和设备 C 的通信范围在 1 跳内。按照图 7.13 所示的通信过程，如果设备 A 开始发送数据包 2 时，设备 C 正在向目的设备 D 转发数据包 1，那么这两个数据包传输就有可能发生冲突。图 7.14 所示为多跳传输中的数据包传输，就反映了这种冲突发生的情形。

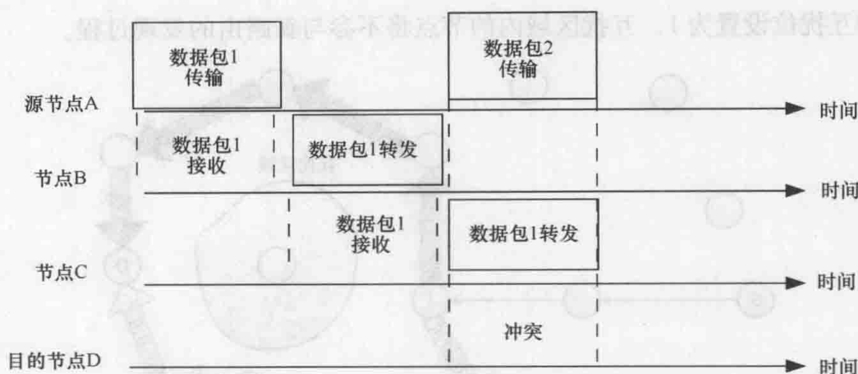


图 7.14　多跳传输中的数据包传输

另一种可能的情形是，节点 B 向节点 C 开始转发数据包 1 时传输数据包 2，这会引起信道竞争。然后，其中一个节点应延迟访问信道，并在准备下一次访问信道之前等待一个随机的时延。如果源节点 A 没有恰当地控制传输时间间隔（如时间间隔太小），随后的数据包传输可能引起更大的时延。在 IEEE 802.15.4 标准中，默认重发数据传输机制对在数据传输之后没有收到期望确认的情况不太有效。如果多跳数据传输涉及较多的中间节点，冲突和信道竞争将会变得更加复杂和不可预知。在设计传输协议时必须考虑多跳数据传输的不确定性。

为保证多跳数据传输的成功，源节点应对数据包传输的时间间隔设置一个最小值，该值应等于数据包从源节点传输到目的节点所需要的时间。如果后面的数据只有在目的节点收到前面的数据之后开始传输，发生碰撞和信道竞争的可能性会很小。最小时间间隔的定义如下：

$$T_{\text{Total}}(L)N_{\text{Hops}} \tag{7.8}$$

式中，T_{Total}（L）为在单跳数据传输中从一节点到另一节点发送 L 字节数据包所需的时间；L 为数据包的大小；N_{Hops} 为多跳数据传输的跳数。两个连续数据包传输的最小时间间隔可以设置在 MAC 层和相关的高层（如网络层和应用层）。

7.6.4.2　多跳数据传输的互扰抑制

若互扰发生，网状拓扑将为 IEEE 802.15.4 网络的部署提供极大的灵活性。如果现有的路由不可用，那么路由协议可以重新找到一条新的多跳数据传输的路由。在某种情况下，大多数无线节点受到干扰时，可以有效切换到另一个空闲信道。但是，随着 IEEE 802.15.4 网络覆盖范围的增加，保持整个 IEEE 802.15.4 网络同步将需要相当大的开销，实现信道切换的问题将随之增加。

图 7.15 和 7.16 给出了发现绕过互扰区域的新路由的互扰抑制方法（Salvatore 和 Yang，2012）。为了操作方便，每个节点存储一个直接邻居列表，并且每个邻居用一个相关的互扰比特位指示其是否受到干扰。详细地说，节点为每个邻居记录丢失的确认包。如果丢失的确认数超过指定的限制，则认为其邻居处于互扰区域并将

相应的互扰位设置为 1。互扰区域内的节点将不参与新路由的发现过程。

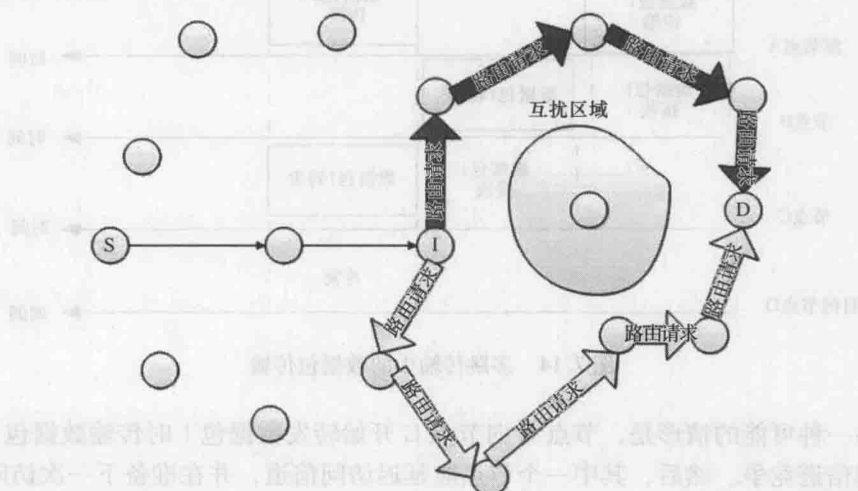


图 7.15　发现互扰后新路由发现过程

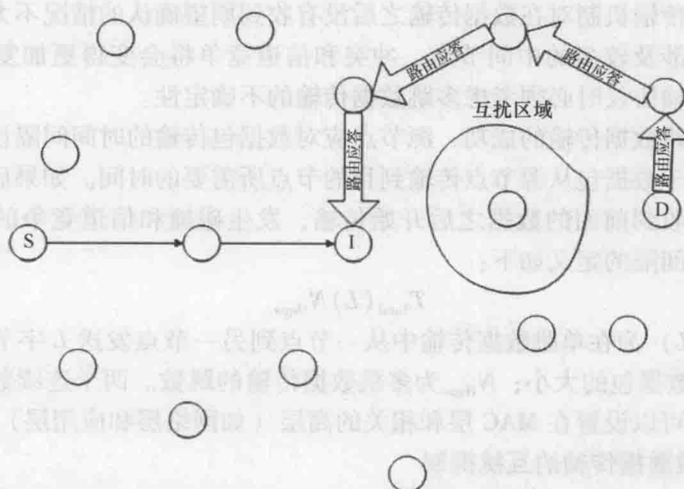


图 7.16　发现互扰后路由应答传播

中间节点仍然有必要向源节点回送一个链路故障报文。于是，源节点停止发送任何数据包并等待一段指定的时间。可以根据网络的大小调整这段时间的大小。只有在中间节点不能发现一条新的到达目的节点路由的情况下，它将向源节点回送一个路由错误报文以便一开始就启动一个新的路由发现过程。如果没有收到路由错误报文，源节点就认为到目的节点的新路由是可用的，然后重新开始向前面的下一跳发送数据包。上述方案也可以应用于检测到的多个互扰区域的情况。

7.7 实验研究

实验研究是研究人员研究干扰影响的更为实用的方法（Jennic，2008）。

7.7.1 单跳传输

Petrova等人的参考文献（2006）给出了IEEE 802.11和IEEE 802.15.4网络共存问题的互扰测试实验，即单跳传输测试，如图7.17所示。

图7.17中，IEEE 802.15.4设备之间和IEEE 802.11b/g设备之间的距离都设置为5m。两个测试系统测试了通信信道之间的各种频段分离，以及不同长度的IEEE 802.15.4数据包，实验结果的PER如图7.18所示。如果IEEE 802.15.4和IEEE 802.11b信道之间的频段分离超过7MHz，那么可以得到可接受的IEEE 802.15.4系统的PER（即大约1%）。显然，数据包长度越大，PER越大。

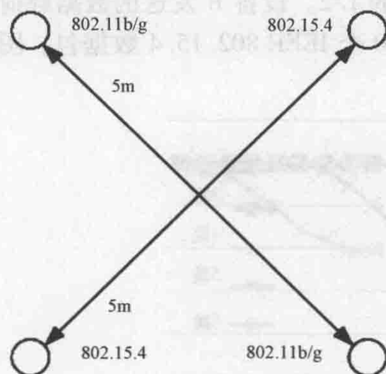


图7.17　单跳传输测试

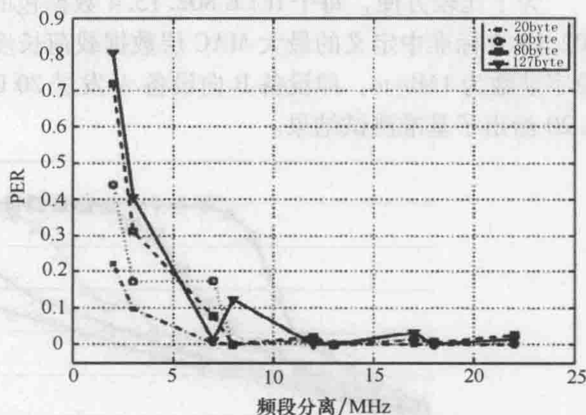


图7.18　具有IEEE 802.11互扰的IEEE 802.15.4的PER

7.7.2 多跳传输

本节实验（Yao，2010）由三个测试组成：基准测试、互扰测试和数据恢复测试。基准测试和互扰测试主要解决基于IEEE 802.15.4的移动自组网在Wi-Fi互扰和没有Wi-Fi互扰情况下的传输性能问题。数据恢复测试旨在评价新路由是否可以改善多跳传输的性能。所有实验都在Jennic JN5139R1平台上完成（Jennic，2009）。

7.7.2.1 基准测试：多跳通信的传输控制

从7.6.4.1节和式（7.8）可以知道，两个连续传输数据包之间的最小传输间隔在任意的中间设备上都必须避免过大。基准测试用来说明传输间隔的设置如何严重影响多跳传输的性能。基准测试中的硬件部署如图7.19所示。



图 7.19 基准测试中的硬件部署

图 7.19 中，目的设备为设备 A；源设备为向设备 A 发送数据的设备 B；用来转发数据的中间设备为位于设备 A 和 B 之间的设备。传输路由事先部署到这些中间设备中。源设备 B 按照图 7.19 所示的跳的顺序（跳 1→跳 2→…→跳 n）向设备 A 发送数据。在这部分测试中，跳数事先指定，从 2 变化到 6。运行在设备 A 中的软件记录接收到的数据量。

为了比较方便，每个 IEEE 802.15.4 数据包的载荷长度设置为 50byte，是 IEEE 802.15.4 标准中定义的最大 MAC 层数据载荷长度的 1/2。设备 B 发送的数据载荷总字节数为 1Mbyte，即设备 B 向设备 A 发送 20 000 个 IEEE 802.15.4 数据包。图 7.20 给出了基准测试结果。

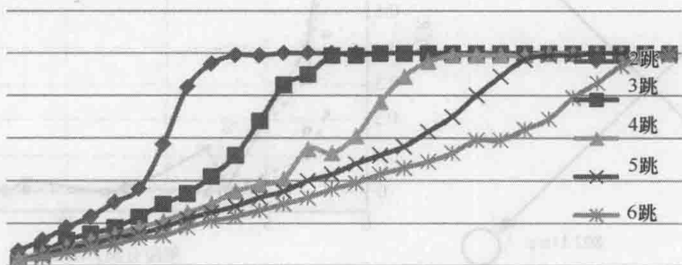


图 7.20 基准测试结果

图 7.20 中，横轴为源设备 B 中两个连续传输数据包之间的传输间隔。纵轴为设备 A 测量到的相应的数据到达率。测试结果验证了到达率的好坏明显和多跳传输的跳数有关。例如，为了获得一个令人满意的 2 跳传输的到达率（超过 99%），最小时间间隔约为 10ms，而 4 跳的多跳传输间隔至少为 19ms。显然，多跳传输中跳数越多，则指定的传输间隔越长。

7.7.2.2 互扰测试

互扰测试旨在研究互扰对多跳传输到达率的影响。在互扰测试中，一个 IEEE 802.11b 路由器靠近其中一个中间设备，并使用固定包速率（如 10packet[⊖]/s、

⊖ packet：包。

100packet/s）广播 IEEE 802.11b 信号。在 IEEE 802.15.4 多跳传输期间，每个中间设备记录成功接收到的数据包数。通过与源设备发送的数据包总数进行比较，就会清楚互扰是如何影响多跳传输的。图 7.21 给出了互扰测试的硬件部署。

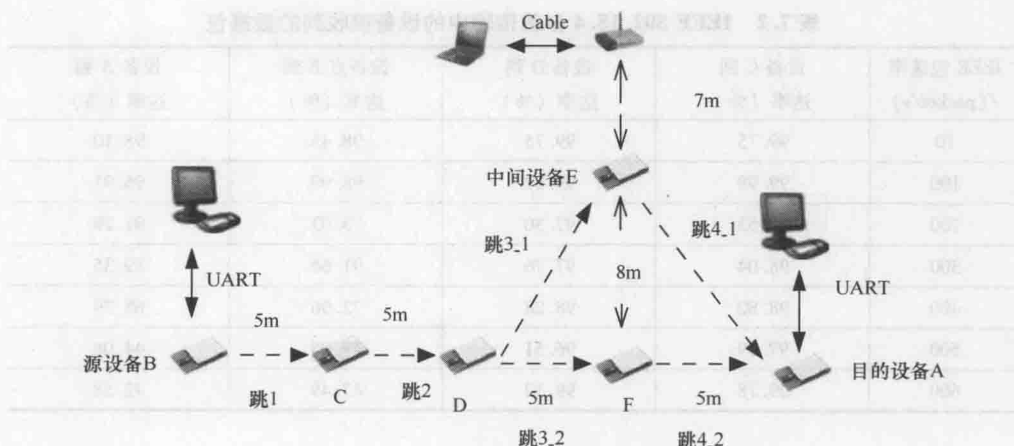


图 7.21　干扰测试的硬件部署

图 7.21 中，工作在信道 13（即 2472MHz）的 IEEE 802.11b Wi-Fi 路由器连接一台笔记本计算机，并与中间设备 E 相隔 7m。在笔记本计算机上安装基于专用软件的包产生器，不断干扰设备 E。在 IEEE 802.15.4 移动自组网络中，按照跳 1→跳 2→跳 3_ 1→跳 4_ 1 的顺序，预先指定 4 跳数据传输。传输间隔设置为 22ms，从基准测试可以知道该传输间隔可以获得大约 99% 的到达率，如图 7.20 所示。IEEE 802.15.4 移动自组网络工作在信道 23（即 2465MHz）。其中心频率与 IEEE 802.11b 路由器使用的通信信道的中心频率相差 7MHz。

在互扰测试中，IEEE 802.11b 无线路由器以从 10packet/s 到 600packet/s 的包速率广播信号。IEEE 802.15.4 数据包的载荷为 50byte。源设备发送的 IEEE 802.15.4 数据包总字节数为 20 000byte。如表 7.2 所示，互扰测试结果表明，当 IEEE 802.11b 信号以大占空比工作时，来自 IEEE 802.11b 无线路由器的互扰能导致 IEEE 802.15.4 移动自组网络到达率大幅下降。这里的到达率是指接收到 IEEE 802.15.4 数据包与源设备 B 发送的数据包的百分比。

显然，位于互扰区域的设备 E 的到达率最先明显下降。最坏的情况是，当无线路由器工作在 600packet/s 时，目的设备 A 测量到的相应的到达率只有 42.58%。

7.7.2.3　数据恢复测试

通过使用一条新路由进行数据恢复测试，即一旦检测到互扰就用设备 F 去替换中间设备 E。数据恢复测试使用的路由为跳 1→跳 2→跳 3_ 2→跳 4_ 2。IEEE

802.11b 无线路由器和设备 F 之间的距离为（8 +7）m =15m。因为物理位置的分离，可以预料 IEEE 802.11b 无线路由器对设备 F 的互扰弱多了。当 IEEE 802.11b 包速率分别为 400packet/s、500packet/s 和 600packet/s 时，目的设备 A 的到达率分别为 95%、86% 和 82%。

表 7.2　IEEE 802.15.4 多跳传输中的设备接收到的数据包

IEEE 包速率 /(packet/s)	设备 C 到达率（%）	设备 D 到达率（%）	设备点 E 到达率（%）	设备 A 到达率（%）
10	99.75	99.75	98.45	98.10
100	99.99	99.87	98.99	96.91
200	97.53	97.30	93.03	91.29
300	98.04	97.76	91.66	89.35
400	98.80	98.28	72.06	68.79
500	97.39	96.51	49.05	44.06
600	99.78	99.12	47.49	42.58

7.8　小结

本章介绍了互扰的定义、互扰产生的原因和一些互扰抑制策略，重点研究了 IEEE 802.11b 和 IEEE 802.15.4 之间的互扰问题。一般地，只有满足两个条件互扰才会发生：无线频率分离很小或分离为零，以及能量干扰强。抑制策略可作如下分类：

● 信道选择。推荐使用信道 25 或信道 26 来避免大多数的 IEEE 802.11b/g 互扰。如果无线系统部署在可控的环境中，那么信道中心频率分离应保留 7MHz 以便保证与 IEEE 802.11 系统共存。

● 物理分离。为了共存有必要保证距 IEEE 802.11 接入点的物理分离至少为 8m。

● 网状组网。如果允许，IEEE 802.15.4 网络可以建构在具有自组织和自愈能力的网状拓扑结构的基础上。

● 网络层频率变化。当互扰发生时切换到一个空闲信道，IEEE 802.15.4 网络可以有效避免性能下降。高层协议（如网络层）通常都支持信道跳频。动态信道选择应根据信道评估（如能量监测、链路质量指示）的结果决定。

● 网络规划。在部署 IEEE 802.15.4 网络之前，可以进行像现场调查这样的初步评估以评估无线频率环境。评估结果将为物理安装提供重要的指导。在系统运行期间，可以周期性地评估无线频率环境以便监测可能发生的互扰的任何变化。

参考文献

Chandra, P., Dobkin, D.M., Bensky, D., Olexa, R., Lide, D., Dowla, F.: Wireless Networking, Know It All. Newnes (2007)

Cuomo, F., Luna, S.D., Monaco, U., Melodia, T.: Routing in ZigBee: Benefits from exploiting the IEEE 802.15.4 association tree. IEEE Int. Conf. Commun., 3271–3276 (2007)

Fakatselis, J.: Processing gain for direct sequence spread spectrum communication systems and PRISM. In: Harris Semiconductor Application Note (1996)

Fakatselis, J.: Processing gain in spread spectrum signals. In: Harris Semiconductor Application Note (1998)

Golmie, N.: Coexistence in Wireless Networks Challenges and System-Level Solutions in the Unlicensed Bands. Cambridge University Press, Cambridge (2006)

Golmie, N., Cypher, D., Rebala, O.: Performance analysis of low rate wireless technologies for medical applications. Comput. Commun. **28**(7), 1266–1275 (2005)

Hwang, L.J., Sheu, S.T., Shih, Y.Y., Cheng, Y.C.: Grouping strategy for solving hidden node problem in IEEE 802.15.4 LR-WPAN. In: Proceedings of First IEEE International Conference on Wireless Internet (WICON), pp. 26–32 (2005)

IEEE Standard 802.11.: IEEE standard for information technology: Telecommunications and information exchange between systems: Local and metropolitan area networks: Specific requirements: Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications (2007)

IEEE Std 802.15.4.: IEEE standard for information technology: Telecommunications and information exchange between systems: Local and metropolitan area networks: Specific requirements part 15.4: Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LRWPANs) (2003)

IEEE.: 802.15.2 definition of coexistence. Available at http://grouper.ieee.org/groups/802/15/pub/2000/Sep00/99134r2P802-15_TG2-coexistenceinteroperabilityandotherterms.ppt (2000)

Jennic.: Co-existence of IEEE 802.15.4 at 2.4 GHz. In: Jennic Application Note (2008)

Jennic.: JN5139 data sheet. Available at http://www.jennic.com/download_file.php?supportFile=JN-DS-JN5139MO-1v5.pdf (2009)

Kang, M.S., Chong, J.W., Hyun, H., Kim, S.M., Jung, B.H., Sung D.K.: Adaptive interference: aware multi-channel clustering algorithm in a ZigBee network in the presence of WLAN interference. In: IEEE International Symposium on Wireless Pervasive Computing (2007)

Koubaa, A., Alves, M., Tovar, E.: IEEE 802.15.4: A wireless communication technology for large-scale ubiquitous computing applications. In: Proceeding of Conference on Mobile and Ubiquitous Systems. Guimarães (2006)

Molisch, A.F.: Wireless Communications. Wiley (2005)

Petrova, M., Riihijarvi, J., Mahonen, P., Labella, S.: Performance study of IEEE 802.15.4 using measurements and simulations. In: Wireless Communications and Networking Conference (WCNC), pp. 487–492 (2006)

Rodriguez, R.: MC1319x coexistence. In: Freescale Semiconductor Application Note, AN2935 (2005)

Salvatore, D., Yang, S.H.: Routing algorithm of WSN under interference environment. In: Wireless Sensor Systems: IET Conference, London (2012)

Shin, S.Y., Park, H.S., Kwon, W.H.: Mutual interference analysis of IEEE 802.15.4 and IEEE 802.11b. Comput. Netw. **51**(12), 3338–3353 (2007)

So, J., Vaidya, N.: Multi-channel MAC for ad hoc networks: Handling multi-channel hidden terminals using a single transceiver. In: Proceedings of the 5th ACM International Symposium on Mobile Ad hoc Networking and Computing, pp. 222–233 (2004)

Thone, G., Allard-Jacquin, P., Colle, P.: ZigBee-WiFi coexistence, white paper and test report (2008)

Won, C., Youn, J.H., Ali, H., Sharif, H., Deogun, J.: Adaptive radio channel allocation for supporting coexistence of 802.15.4 and 802.11b. IEEE Veh. Technol. Conf. **4**, 2522–2526 (2005)

Yao, F.: Interference mitigation strategy design and applications for wireless sensor networks. PhD thesis, Loughborough University, Loughborough (2010)

Yao, F., Yang, S.H.: Mitigating interference caused by IEEE 802.11b in the IEEE 802.15.4 WSN within the environment of smart house. In: Proceedings of the 2010 IEEE International Conference on System, Man, Cybernetics. IEEE, Istanbul, Turkey, pp. 2800–2807 (2010)

Yilmaz, O.: Propagation simulation for outdoor wireless communications in Urban areas. Available at www.ee.bilkent.edu.tr/grad/ms-thesis/yilmaz-ms.pdf (2002). Accessed Aug 2011

ZigBee, A.: ZigBee and wireless radio frequency coexistence. Available at http://www.zigbee.org (2007). Accessed June 2012

第 8 章　传感器数据融合和事件检测

关键词：数据融合　模式提取　数据挖掘　网内数据库

8.1　引言

传感器数据中经常含有大量的冗余信息，即使采用专业的数据分析方法也难以解释数据的含义。传感器数据常常还包含噪声，很难将其和“真正的”数据分开。此外，除非将传感器数据与时间和位置信息关联，否则传感器数据没有意义。本章的主要内容是介绍使传感器数据可用所需的技术和步骤。

8.1.1　传感器数据特征

相对于传统数据而言，传感器网络数据具有其独有的特征，为管理和处理此类数据带来了挑战。

8.1.1.1　数据流特性

传感器数据最好按连续到达的数据流建模而不是按持续关系建模。数据流与传统数据的不同之处如下（Yang 等，2010）：

- 传感器数据自动生成，以多路、连续、时变的方式传输。因此，传感器数据随着时间的推移而增加，且数据总量可能没有限制。而传统数据则是由人工输入，永久或持续地存储在数据库中，且容量有限。
- 数据流是按时间排序的数据，或者具有显式的时间戳或者基于隐式的到达排序（Kim 等，2005）。而传统数据除非有明确规定否则通常都不是按时间排序。

因此，传感器数据流的特征给传感器数据处理带来了挑战，如无限增长的数据存储、连续加载和持续查询。

8.1.1.2　强时空相关性

传感器通常是按照一定的密度进行部署的，这样能够使传感器覆盖整个监测区域。因此，大部分传感器网络的各节点间的读数会表现出时间和空间上的相关性（Silberstein 等，2007）。更具体地说，强时空相关性使传感器数据具有如下特征：某一时刻观测到的读数不仅对下一时刻观测到的读数具有高度预测指示性，还对附近设备的读数具有指示性（Jeffery 等，2006）。

不管怎样，强时空相关性具有潜在的优点。强时空相关性的这些优点可以用来估计丢失或损坏的数据（Chok 和 Gruenwald，2009）、监测偏值、提高传感器数据的质量、进行数据抑制（Silberstein 等，2007）、减少网络中的数据传输，从而降

低能耗。然而，在相关性确定、相关性建模和保持相关性数据更新等方面还面临着挑战。

8.1.1.3 数据冗余

在传感器数据中，强时空相关性会导致数据库中的数据具有大量的冗余。然而，冗余可以用来预测丢失值和检测偏值。一定程度的冗余可以提高数据库查询结果的准确性。处理冗余的传感器数据并不是简单地删除掉冗余数据，而是要保留数据的重要信息且不会产生不必要的存储需求。

8.1.1.4 噪声

传感器设计的目标是要低功耗和低成本。然而，这会导致传感器的精度受限。除了设计问题，传感器通常部署在严酷的环境中，会受到潜在的环境干扰。因此，传感器可能会因火灾等紧急情况而出现内部故障或损坏。研究表明，传感器数据通常含有错误（由传感器功能引起）和噪声（由其他环境干扰引起）（Elnaharawy 和 Nath，2003）。这些特征表明，在把传感器数据存储到数据库之前，应先对传感器数据进行清理。

8.2 传感器数据融合技术

传感器数据的融合过程包括三个阶段：预处理、数据挖掘和后处理。图 8.1 给出了从原始数据提取信息的全部过程（Tan，2006）。

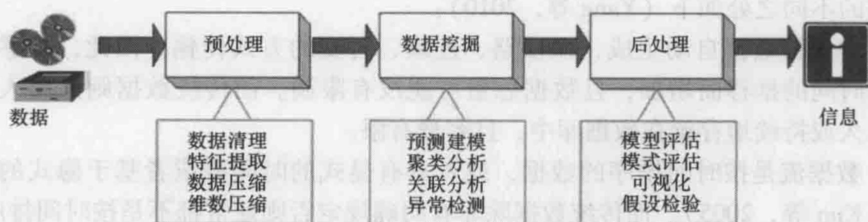


图 8.1 从原始数据提取信息的全部过程（Tan，2006）

8.2.1 传感器数据预处理

传感器网络中的数据质量问题，近期受到越来越多的关注。传感器数据通常包含噪声（Elnahrawy 和 Nath，2003）、偏值（Basu 和 Meckesheimer，2007）和丢失值（Allison，2001）。如图 8.2 所示，引起这些数据质量问题的原因包括，（1）传感器内部误差，（2）传感器部署所处的严酷环境，（3）无线传输过程中数据的损毁和丢失。数据预处理包括，数据清理、偏值检测、丢失值恢复、数据压缩、维数压缩和数据预测等。

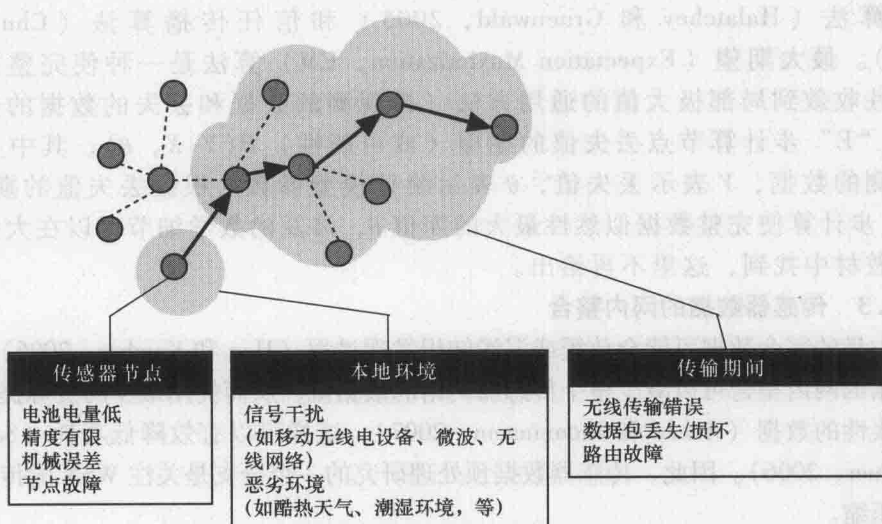


图 8.2　传感器网络中可能引起数据质量问题的因素

8.2.1.1　传感器数据清理

目前已有多种方法用于传感器数据清理，包括贝叶斯理论、神经网络、小波、卡尔曼滤波和加权移动平均。由于计算能力有限，传感器很难实现贝叶斯理论、神经网络和小波方法。因此本章只讨论卡尔曼滤波和加权移动平均这两种方法。

Zhuang 等人（2007）提出了一个基于传感器数据清理的智能加权移动平均方法，该方法包括以下三个步骤：

● 第一步，通过预测范围找出重要数值；

● 第二步，通过在单一传感器上进行传感器测试和邻居测试，来增加重要数值的置信度；

● 第三步，在汇聚节点执行加权移动平均算法。

这种方法采用卡尔曼滤波和线性回归进行范围预测。在预测范围内的值被称为“重要值”，并在第二步中计算它的置信度。最后，在汇聚节点结合时间平均和空间平均进行移动加权平均。

8.2.1.2　丢失值恢复

对于解决网络数据丢失的问题，传统的方法是，在接收方向发送方发送一个重传请求之前，将等待一个预定义的时间周期；或者是如果没有收到来自接收方的确认，则自动重传数据包。然而，在传感器网络中使用这种方法主要有两个缺点：（a）会增加传感器的功耗；（b）会增加由查询产生的结果延迟（Halatchev 和 Gruenwald，2005）。因此，在处理传感器数据丢失的现有研究中，重点是使用与丢失的传感器数据有关的传感器中可用的数据，来估计或恢复丢失的数据。

目前已提出了多种估计方法，如最大期望算法（Moon，1996年）、关联规则算法（Halatchev 和 Gruenwald，2005）和信任传播算法（Chu 等，2005）。最大期望（Expectation Maximization，EM）算法是一种使完整数据似然性收敛到局部极大值的通用方法（即观测的数据和丢失的数据的似然性）。“E”步计算节点丢失值的期望（或可能性）$P(Y|X, \theta)$，其中 X 表示观测的数据，Y 表示丢失值，θ 表示统计模型参数。根据丢失值的期望，“M”步计算使完整数据似然性最大的期值 θ，涉及的数学细节可以在大多数统计教材中找到，这里不再给出。

8.2.1.3 传感器数据的网内整合

大量的冗余数据可能会放缓或混淆知识发现过程（Han 和 Kamber，2006）。冗余数据的网内整合可以减少整个传感器网络的数据流，从而使用最少的资源提取最具代表性的数据（Akcan 和 Brönnimann，2007），这样可以有效降低功耗（Santini 和 Römer，2006）。因此，传感器数据预处理研究的一个分支是关注 WSN 的传感器数据压缩。

最简单的情况是，当原始数据大于预定义的阈值时，求出原始数据的平均值并记录该平均值。表 8.1 给出了结构化查询语言（Structured Query Language，SQL）中的平均整合查询语句，AVG 为传感器采集的平均温度值。如果该平均值大于阈值，则通过“Having AVG”，发送平均值，采样周期为 30s。

Akcan 和 Brönnimann（2007）提出了一种加权网内采样算法，来获得确定性（更小、更典型）样本而非原始冗余数据。与随机采样相比，加权采样的优势在于它可以保证每个节点的数据都有相同的机会归属最终样本，而独立于它的网络来源。

表 8.1 SQL 中的平均整合查询语句

SELECT AVG (temperature), FROM Sensors
WHERE floor = 6
HAVING AVG (temperature) > threshold
SAMPLE PERIOD 30s

基于预测数据压缩的策略（Santini 和 Römer，2006）不是有选择地对网络节点进行采样，而是将预测方法部署在传感器和汇聚节点。这样，传感器只需发送偏离预测值的数据。更具体地说，方法如下：

- 在汇聚节点和传感器节点运用预测模型 G 来获得下一时刻传感器读数的估计值 $\overline{X}^{t+1} = G(X^t)$。
- 在传感器节点，如果 $|X^{t+1} - \overline{X}^{t+1}| > \varepsilon$，就向汇聚节点发送实际传感器读数。其中，$X^{t+1}$ 为下一时刻传感器的实际读数，ε 为容忍误差。

● 否则，汇聚节点使用传感器读数的估计值。

8.2.2　传感器数据挖掘

数据挖掘的目的是从数据中提取模式。传统的数据挖掘技术（Han 等，2001）通常指的是数据挖掘工具，包括决策树、基于规则的分类器、人工神经网络、最邻近节点、朴素贝叶斯、支持向量机、逻辑回归。其中大部分最初被用于中心数据仓库。

传感器数据挖掘主要致力于分布式网内数据挖掘。大多数研究人员提出将层次化网络拓扑结构用于传感器数据挖掘。Bontempi 和 Borgne(2005) 提出了一种用于传感器数据挖掘的二层结构，这是一种传感器数据挖掘的自适应模块化结构，如图 8.3 所示。

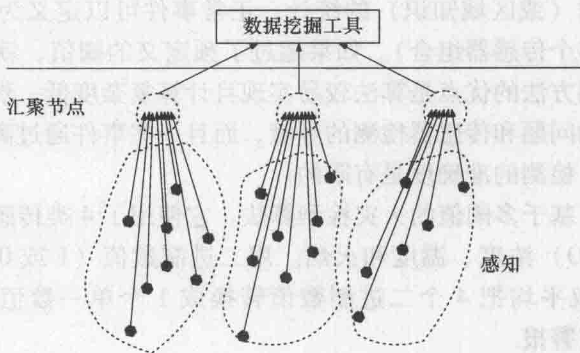


图 8.3　一种传感器数据挖掘的自适应模块化结构

底层由用虚线表示的汇聚节点的构成，完成用黑点表示的相邻传感器节点的聚合。汇聚后的信号被送到上一层进行数据挖掘。在这里要完成的感知任务有分类、回归和预测等。这个结构在 WSN 拓扑中引入了汇聚节点层，每个汇聚节点都作为一些传感器节点的簇头。

8.2.3　传感器数据后处理

数据处理包括模式评估、模型评估、数据可视化/表示等。通过这一步可以把传感器数据挖掘的结果和特定的应用进行关联。数据可视化可以基于计算机图形、统计方法，或基于用户交互技术。这个问题超出了本书讨论的范畴，这里略去。

8.3　事件检测

事件检测可以描述如下形式：

给定一组一定时间内获得的测量数据，表示为 $D=\{z_t \mid t=1,2,3,\cdots n\}$，事件检测就是找到感兴趣的事件的发生时间 t，即不同于正常行为模式的数据的发生时间。

因此，事件检测通常的目的有以下两个：

● 确定是否发生了感兴趣的事件；

● 描述事件的特征（如时间、受影响的区域、事件的类型及其严重性）。

传感器网络应用中已确定了两类事件检测的方法（Yang 等，2012）：基于阈值的事件检测和基于时空模式的事件检测。

8.3.1 基于阈值的事件检测

基于阈值的事件检测方法是事件发生时会引起传感器读数发生变化的一种直观反映的方法，如物体移动会导致加速度读数增加、明火会导致温度读数上升。因此，基于历史数据（或区域知识）的统计，正常事件可以定义为一个阈值（如最大值、增长率及多个传感器组合）。如果超过了预定义的阈值，就会引起警报。基于阈值的事件检测方法的优点是算法较易实现且计算复杂度低。然而，跨越阈值高度依赖具体检测的问题和传感器检测的环境，而且一些事件通过离散阈值不能完全被捕获到。因此，检测的准确度是有限的。

图 8.4 给出了基于多阈值的火灾检测算法。它使用了 4 类传感器读数：烟雾浓度、一氧化碳（CO）浓度、温度和火焰。用二进制数值（1 或 0）表示传感器读数状态。采用加权平均把 4 个二进制数值转换成 1 个单一数值。如果该值大于 50%，就触发火灾警报。

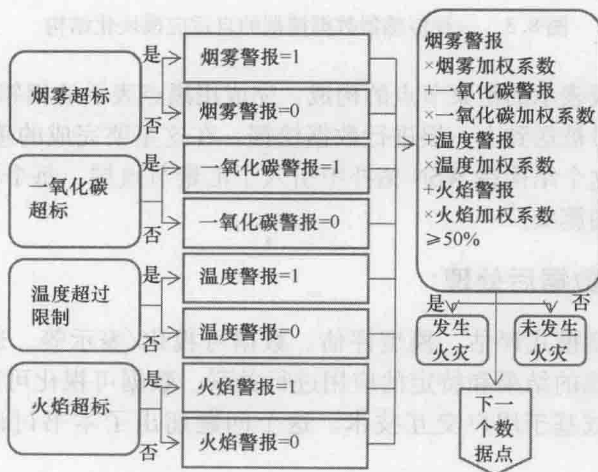


图 8.4 基于多阈值的火灾检测算法

8.3.2　基于时空模式的事件检测

与基于阈值的事件检测不同，基于时空模式的事件检测是指在监测区域内发生的事件会使网络节点传感器读数具有一定的时空模式。例如，一个气体泄漏事件可以被表征为一种从泄漏源到周围区域呈现增长趋势的传感器读数空间分布。可以将感兴趣的事件定义为时间模式（Mukherji 等，2008）、空间模式（Xue 等，2006）或时空模式，然后就可以将事件的检测问题转化为模式匹配问题。

图 8.5 所示为基于空间感知的事件检测，是一个空间模式匹配的例子。这个例子将左侧的现场传感器数据中提取的模式与中间的事件的预定义模式进行比较。如果两者不匹配，则检测结果为正常；否则，表示事件被检测到。它经常用于表示时空模式的等高线地图（Xue 等，2006），是一种用等高线（轮廓线）来表示海拔和地表形态的地图。沿着一条等高线，传感器读数为一个恒定值。

基于时空模式的事件检测方法的优点是，通过考虑上下文信息及传感器数据中普遍存在的时空相关性来改进事件检测的准确度。但是，该方法仍然存在以下缺点：

- 增加了复杂度。因为在模式匹配的过程中，它包含了整个网络的数据。
- 难以确定合适的模式来表示事件的特征。如果定义成静态模式，灵活性就差；如果定义成含有用户指定因素的模式，那么调整这些因素就会遇到和调节阈值类似的问题。

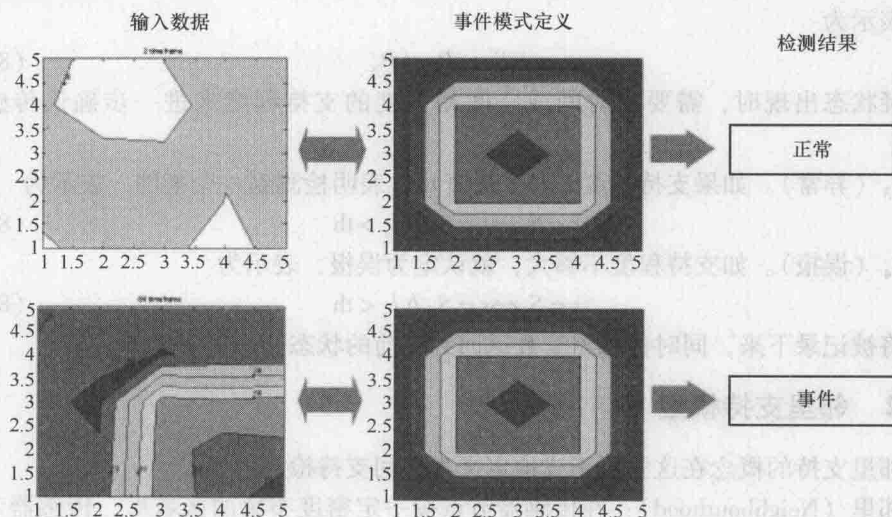


图 8.5　基于空间感知的事件检测

8.4 具有邻里支持的通用传感器状态模型

8.4.1 通用传感器状态模型

无论传感器测量什么，传感器可能处于下面4种可能状态中的一个：正常、可疑、异常和误报。这4种状态之间的转换如图8.6所示，可如下描述：

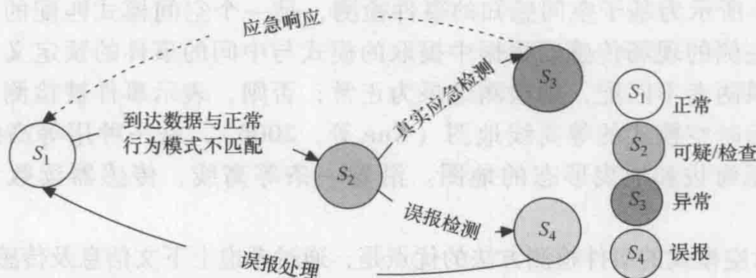


图8.6 通用传感器状态模型

S_1（正常）。如果从现场传感器读数中提取的模式P_L与预定义的行为正常模式P_N相匹配，则s为正常状态，表示为

$$s \in S_1 \Leftrightarrow P_L \approx P_N \tag{8.1}$$

S_2（可疑/检查）。如果P_L与行为正常模式P_N不匹配，则表示出现了可疑状态，表示为

$$s \in S_2 \Leftrightarrow P_L \neq P_N \tag{8.2}$$

当可疑状态出现时，需要用时间或空间相关度的支持程度来进一步确认传感器状态。

S_3（异常）。如果支持程度l_s大于阈值th，表明检测到一个事件，表示为

$$s \in S_3 \Leftrightarrow s \in S_2 \wedge l_s > \text{th} \tag{8.3}$$

S_4（误报）。如支持程度不够大，就认定为误报，表示为

$$s \in S_4 \Leftrightarrow s \in S_2 \wedge l_s < \text{th} \tag{8.4}$$

误报将被记录下来，同时传感器读数返回到以前的状态。

8.4.2 邻里支持模型

邻里支持的概念在这里更正式地定义为空间支持检测的例子。

邻里（Neighbourhood）：在传感器节点按一定密度布置的区域里，传感器节点s_i的邻里包括所有与s_i距离小于等于半径r的传感节点，表示为$N_{s_i} = \{s_j \mid \text{dis}(s_j, s_i) \leqslant r\}$。其中，dis（$s_j$，$s_i$）为传感器节点$s_j$到$s_i$的距离，并且假定传感器节点在部署阶段或通过基于RF的信标知道自己的地理位置信息。

邻里支持（Neighbourhood Support）：邻里支持指当传感器节点检测到可疑状态时它从邻里得到的支持程度，用 NS 表示。直观地，可以将邻里传感器节点看做是证人，能够确认或否认传感器节点检测到的可疑状态。它可以由阈值或等高线地图来实现。

8.5 基于传感器状态模型的事件检测

传感器状态模型的状态转换，既可以基于阈值模式又可以基于时空模式。因此，状态转换可用于这两种模式的事件检测。

8.5.1 基于阈值的事件检测

对于基于阈值比较的状态转换，传感器的通用状态模型可以如下描述：

S_1（正常）。对于任意的具有 m 种传感器的节点，如果它的上升率 RR_i 在阈值 TH_i 范围内，则每个传感器状态 z_i 是正常的，可表示为 $z_i \in S_1 \Leftrightarrow RR_i \leqslant TH_i$，$i=1, 2, \cdots, m$。如果所有 m 种传感器是正常的，则节点 s 的所有状态是正常的，可表示为

$$s \in S_1 \Leftrightarrow z_1 \in S_1 \wedge z_2 \in S_1 \wedge \cdots \wedge z_m \in S_1 \tag{8.5}$$

S_2（可疑/正在检查）。当上升率超过阈值 TH_i，则认为每个传感器的状态为可疑状态，可表示为 $z_i \in S_2 \Leftrightarrow RR_i > TH_i$，$i=1,2,\cdots,m$。当 m 种传感器中的任何状态可疑时，则节点为可疑状态，可表示为

$$z_i \in S_2 \Leftrightarrow z_1 \in S_2 \vee z_2 \in S_2 \vee \cdots \vee z_m \in S_2 \tag{8.6}$$

当可疑状态出现时，系统就会检测邻里支持，邻里支持定义为处于可疑状态的邻里数 N_{S_2} 与所有邻里总数 N_n 的比，可表示为 $NS=\dfrac{N_{S_2}}{N_n}$。

S_3（异常）。如果邻里支持大于阈值 th，则表明检测到一个事件，可表示为

$$s \in S_3 \Leftrightarrow s \in S_2 \wedge NS > th \tag{8.7}$$

S_4（误报）。如果邻里支持不够大，它将被视作一个偏值。偏值将被记录，同时传感器返回到以前的状态，可表示为

$$s \in S_4 \Leftrightarrow s \in S_2 \wedge NS < th \tag{8.8}$$

8.5.2 基于时空模式的事件检测

在式（8.1）和式（8.2）所表示的通用传感器状态模型中，传感器行为的当前模式 P_L 和正常模式 P_N 可以用等高线地图的形式表示（Xue 等，2006）。这个等高线地图就是整个网络的传感器读数的分布。将 P_L 和 P_N 分别重命名为从现场传感器读数中提取的等高线地图 C_L 和预定义等高线地图事件模式 C_E。对于基于等高线地图匹配的状态转换，传感器的通用状态模型可以分别地表示为以下几种情况：

S_1（正常）。如果从现场传感器读数中抽取出的等高线地图 C_L 与任何预定义等高线地图事件模式 C_E 不匹配，那么当前状态 s 为正常状态，可表示为

$$s \in S_1 \Leftrightarrow C_L \neq C_E \tag{8.9}$$

S_2（可疑/检查）。如果 C_L 与等高线地图事件模式 C_E 匹配，则表示发生了可疑状态，可表示为

$$s \in S_2 \Leftrightarrow C_L = C_E \tag{8.10}$$

如果有可疑状态发生，系统就会检查匹配是否持续了一定的连续时间周期 T。

S_3（异常）。如果可疑状态没有持续一定的连续时间周期 T，且具有邻里支持，则表示检测到了一个事件，可表示为

$$s(t) \in S_3 \Leftrightarrow s(t-T+1,\cdots,t) \in S_2 \tag{8.11}$$

式中，t 为检测时间。

S_4（误报）。如果可疑状态没有持续一定的连续时间 T，并且/或者对可疑状态没有充分的的邻里支持，就认为是误报，即为偏值，可表示为

$$s(t) \in S_4 \Leftrightarrow s(t) \in S_2 \wedge \exists s(t) \in S_1, t = \{t-T+1, t-T+2, \cdots, t\} \tag{8.12}$$

8.6 传感器网络数据库

传感器网络数据库（Govindan 等，2002）允许用户向传感器网络发出查询并获得响应，就好像传感器网络是一个数据库系统。由于数据是由单个传感器节点生成并存储在单个传感器节点的，因此传感器网络数据库是一个分布式数据库。传感器网络数据库和传统的分布式数据库最根本的区别在于，传感器网络数据库的数据是在有需求时产生的，即因用户的请求而生的。这一特性被称为数据库操作者的网内实现。当用户向网络发起查询时，该查询请求被传输到整个传感器网络，并传送到相关的传感器节点。作为该查询请求的响应，相关节点生成与查询相匹配的数据记录，并经由网络把记录回送给用户。本书第12章将介绍 WSN 与因特网连接，以及从这一特殊的分布式数据库获取数据的细节。

8.7 小结

传感器数据具有一些特殊的特性。本章总结了它们的数据流特性、强时空相关性、冗余、误差和含噪特性。对于传感器数据的管理和处理所面临的挑战，应妥善解决。本章简要介绍了传感器数据融合技术，将它划分为预处理、数据挖掘和后处理。事件检测是传感器数据融合的主要目的之一。本章把事件检测方法分为基于阈值和基于时空模式两大类，并提出了实现这两种方法的传感器状态模型。传感器网络数据库与传感器数据融合密切相关。在本章的结尾部分介绍了传感器网络数据库的概念。本章省略了传感器数据挖掘和传感器数据查询的细节，因为可以基于传统

的数据挖掘和数据查询技术对其进行开发。

参考文献

Allison, P.D.: Missing Data Thousand Oaks. Sage Publications, CA (2001)

Akcan, H., Brönnimann, H.: A new deterministic data aggregation method for wireless sensor networks. Elsevier J. Sig. Process. **87**(12), 2965–2977 (2007)

Basu, S., Meckesheimer, M.: Automatic outlier detection for time series: an application to sensor data. Knowl. Inf. Syst. **11**(2), 137–154 (2007)

Bontempi, G., Borgne, Y. L.: An adaptive modular approach to the mining of sensor network data. In: Proceedings of 1st International Workshop on Data Mining in Sensor Networks as part of the SIAM International Conference on Data Mining (Newport Beach, CA, 21–23 April 2005), pp. 3–9. SIAM Press (2005)

Chok, H., Gruenwald, L.: An online spatio-temporal association rule mining framework for analysing and estimating sensor data. In: Proceedings of the 2009 International Database Engineering and Applications Symposium, pp. 217–226. Cetraro, Calabria, Italy (2009)

Chu, F., Wang, Y., Parker, D.S., Zaniolo, C.: Data cleaning using belief propagation. In: Proceedings of the 2nd international workshop on Information quality in information systems, pp. 99–104. Baltimore, Maryland, (2005)

Elnahrawy, E., Nath, B.: Cleaning and querying noisy sensors. In: Proceedings of 2nd ACM International Conference on Wireless Sensor Networks and Applications, pp. 78–87. San Diego, CA, USA, (2003)

Govindan, R., Hellerstein, J., Hong, W., Madden, S., Franklin, M., Shenker, S.: The sensor network as a database. Technical Report 02-771, Computer Science Department, University of Southern California (2002)

Halatchev, M., Gruenwald, L.: Estimating missing values in related sensor data streams. In: Proceedings of the International Conference on Management of Data, pp. 83–94. Goa, India (2005)

Han, J., Kamber, M., Pei, J.: Data mining concepts and techniques. Morgan Kaufmann, MA, USA (2011)

Jeffery, S. R., Alonso, G., Franklin, M. J., Hong, W., Widom, J.: A pipelined framework for online cleaning of sensor data streams. In: Proceedings of the 22nd International Conference on Data Engineering, pp. 140–143. Atlanta, GA (2006)

Kim, C.H., Park, K., Fu, J., Elmasri, R.: Architectures for streaming data processing in sensor networks. In: Proceedings of the 3rd ACS/IEEE International Conference on Computer Systems and Applications, p. 59. Washington, DC (2005)

Moon, T.K.: The expectation maximization algorithm. IEEE Sig. Process. Mag. **13**, 47–60 (1996)

Mukherji, A., Rundensteiner, E.A., Brown, D.C., Raghavan, V.: SNIF TOOL: Sniffing for patterns in continuous streams. In: Proceedings of the 17th ACM Conference on Information and Knowledge Management, pp. 369–378. Napa Valley, California, USA (2008)

Santini, S., Römer, K.: An adaptive strategy for quality-based data reduction in wireless sensor networks. In: Proceedings of the 3rd International Conference on Networked Sensing Systems, pp. 29–36. Chicago (2006)

Silberstein, A., Braynard, R., Filpus, G., Puggioni, G., Gelfand, A., Munagala, K., Yang, J.: Data-driven processing in sensor networks. In: Proceedings of 3rd Biennial Conference on Innovative Data Systems Research (CIDR), pp. 10–21. Asilomar, California (2007)

Tan, P.: Knowledge discovery from sensor data, available online at: http://www.sensorsmag.com/sensors/article/articleDetail.jsp?id=317466 (2006)

Xue, W., Luo, Q., Chen, L., Liu, Y.: Contour map matching for event detection in sensor networks. In: Proceedings of the ACM SIGMOD international Conference on Management of Data, pp. 145–156. Chicago, USA, (2006)

Yang, Y., May, A., Yang, S.H.: Sensor data processing for emergency response. Int. J. Emergency Manage. **7**(3/4), 233–248 (2010)

Yang, Y., May, A., Yang, S.H.: A generic state model with neighbourhood support from wireless sensor networks for emergency event detection. Int. J. Emergency Manage. **8**(2), 135–152 (2012)

Zhuang, Y., Chen, L., Wang, X.S., Lian, X.: A weighted moving average-based approach for cleaning sensor data. In: Proceedings of 27th International Conference on Distributed Computing Systems (ICDC'07), pp. 38–45. Toronto (2007)

第 9 章　无线传感器网络安全防御

关键字：安全　拒绝服务攻击

9.1　开放式系统互联安全防御的基本概念

国际电信联盟通信标准化委员会（International Telecommunication Union-Telecommunication Standardization Sector，ITU-T）X. 800 建议书给出了 OSI 的安全体系结构，其中包括安全需求和实现这些需求所需要的方法。X. 800 建议书中用到了以下定义：

● 安全攻击，威胁机构或个人信息安全的行为。

● 安全机制，设计用于检测、预防安全攻击或者恢复系统的机制。

● 安全服务，采用一种或多种安全机制以抵御安全攻击、提高机构的信息系统安全和信息传输安全的服务。

安全攻击包括被动攻击和主动攻击。被动攻击的目的是窃听或利用系统中的信息，但并不会影响系统运行。主动攻击试图改变系统资源、性能参数或影响系统操作，或者至少是降低系统性能。

下面列出了 X. 800（ITU-T，1991）中定义的安全机制：

● 密码学，运用某种算法将数据转换成不可知形式的方法，用于隐藏其真实内容，以阻止漏检的恶意篡改或未授权的使用。

● 加密，将数据转换成密文的过程。

● 数字签名，附加在数据单元之后的数据，以使得数据单元的接收方能证明数据源和数据单元的完整性，并防止伪造。

● 访问控制机制，防止未授权用户使用资源的各种机制，包括阻止以未授权形式使用资源的行为。

● 数据完整性机制，用于保证数据不被非法改变或破坏的各种机制。

● 认证交换，通过信息交换来保证实体身份的各种机制。

● 流量填充，伪造通信数据或伪造数据单元或伪造数据单元中的数据。

● 路由控制，在路由过程中，为了选择或避免特定的网络、链路或中继而使用的规则。

● 公证，利用可信的第三方对数据进行注册以保证数据的性质的准确性，如数据的内容、数据源、时间及交付。

安全机制是用来实施安全服务的机制，以保证系统或数据传输足够的安全。

X. 800 建议书将安全服务分为以下几类：

- 认证，认证服务与保证通信的真实性有关，如实体身份的认证或接收信息的信息源的认证。例如，使用网络银行服务时，客户端和银行端都应该保证信息源是它们所声称的信息源，并且都能够确定对方的身份。数据认证最常见的方法，就是利用只有收发双方才持有的密钥对数据进行加密。数据接收者利用正确的密钥核对接收到的加密数据，并且只有通过正确密钥加密过的数据才被认为是可靠的数据。
- 访问控制，是控制指定资源的访问、访问的条件和级别及用户可以进行的访问。在使用网络银行服务的例子中，用户可以有权查看他的账户余额，但不允许对账户余额做任何更改或对账户做任何交易。访问控制技术对认证过的实体访问权限划分成不同的级别。其中用户名和口令控制是最基本的访问控制技术。
- 保密性，指使信息保密防止未授权的第三方查看任何通信内容。一个提供保密性服务的系统，必须保护数据不会被未授权的实体直接或间接地访问。直接访问包括未授权实体对数据的拦截和查看。间接访问包括未授权实体使用流量分析的方式获得通信流量模式并提取通信内容。保证保密性最基本的方法就是数据加密技术。
- 数据完整性，保证数据在合法用户没有检测的情况下不会被未授权的实体进行修改、插入、删除或重放操作。信息加密、信息认证码及哈希函数是三种已有的保证信息不会被恶意篡改的方法。
- 不可抵赖性，在通信过程中，防止参与通信的任一实体进行否认的行为。不可抵赖性与收发双方都有关联，可以证明发送的消息是由特定方发送或接收的。在网络银行的实例中，不可抵赖性可以防止出现这种情况，用户已经进行了交易，但是事后否认进行了交易。数字签名及公证是用于不可抵赖性服务的两种最基本的方法。
- 可用性服务，保护系统以确保它的可用性，特别针对拒绝服务（Denial-of-Service，DoS）攻击。可用性服务关注的是对提供服务系统的保护，保护其不会被攻击者通过永久删除可用服务或间断性地降低可用性级别进而将其删除的方式对这些系统资源进行覆盖操作。恶意用户采用了许多方法来降低服务的可用性，这些方法统称为 DoS 攻击。

针对各种攻击和防止攻击所需的攻击与安全服务机制见表 9.1，可以看出针对任何攻击至少有一种安全服务机制可以用来防御特定的攻击。

表 9.1 攻击与安全服务机制

安全服务	攻击					
	信息内容发布	否认参与	伪装	重放	信息修改	拒绝服务
认证			√			
访问控制			√			
保密性	√					
完整性				√	√	
非拒绝		√				
服务可用性						√

9.2 无线传感器网络安全防御的挑战

与 Ad-hoc 无线网络和其他无线网络类型相比，WSN 具有很多独特特点。当考虑 WSN 的安全性时，不能直接使用传统网络安全技术（Perrig 等人，2004 年）。首先，大规模的传感器网络很可能由上千的传感器节点构成，并且为了能够保证传感器网络低成本的优势，在这些节点中，典型的传感器节点在能量、计算及通信能力方面都会受到限制。其次，无线传感器节点可以遍布于广泛的地理区域，从而存在意外的物理攻击的危险。最后，传感器网络与人类社会及周边环境之间的交互，也带来了新的安全危险。

传统网络中的端到端的安全性问题，如信息的可靠性、完整性和保密性，通常是利用如安全套接层（Secure Socket Layer，SSL）这样的端到端的安全机制来解决的。这种方法需要一种健壮的密钥交换和分配方案。作为资源有限的网络，WSN 的传感器节点在存储和计算方面的能力都是有限的，因此，密钥交换和分配方案必须简单、易于执行。由于传感器节点的硬件通常不能存储大量的加密密钥，因此大部分的通信节点无法实现端对端加密。此外，WSN 中占主导地位的通信模式是多对一的模式，如多个传感器节点对一个汇聚节点或基站。本书第 8 章介绍的数据融合、冗余消除及数据压缩，都需要中间节点来实现信息内容的访问、修改和压缩，从而降低通信成本。所以，在传感器节点和基站之间使用端到端安全机制以保证信息的安全性是不可行的（Du 和 Chen，2008）。对于大规模的 WSN，无法保证每一个传感器节点不受到物理和逻辑攻击。进而，传感器节点的大面积分布使得传感器节点暴露在那些能够捕获和改编传感器节点的非法用户面前。它们也可以诱导 WSN 接受自己的传感器节点作为合法的节点。一旦在 WSN 内部部署了一些恶意节点，非法用户就可以在 WSN 内部发起攻击（Chan 和 Perrig，2003）。WSN 与人类和环境的交互使现场监视成为可能。例如，一幢房子外或是一个传感器覆盖区域安装一些

无线接收器就可以实现对房屋内部或是传感器区域的监视，从而获取相关的详细信息。攻击者可以通过访问存储的传感器数据、查询或监听 WSN，来获得访问敏感信息的机会。攻击者也可以利用对 WSN 的远程访问来获取大量信息而不需要现场监视。

总而言之，对于以上提出的 WSN 中特有的安全挑战，人们需要设计专门的安全技术。

9.3 无线传感器网络面临的攻击分类

WSN 面临的攻击可以有多种分类方式，如根据攻击者的位置、攻击者的能力、攻击的协议层及攻击的目的。

WSN 面临的攻击可以分为外部攻击和内部攻击。在传感器网络中，外部攻击者不能访问大部分已加密的信息，而内部攻击者可以访问部分关键信息和获得某些其他节点的信任。内部攻击者可以将它们自己的传感器节点接入到网络中，并诱导 WSN 接受它们作为合法节点；或者当它们捕获并重新编写节点时，可以对可修改的节点声称多重身份。一旦控制了 WSN 内部的几个节点，内部攻击者就能从 WSN 内部实施各种攻击。典型的内部攻击是伪造传感器数据、从传感器网络读数提取专用的感知信息及拒绝服务。内部攻击更难以检测和防御（Du 和 Chen，2008）。外部攻击在到达 WSN 之前需要穿过网关，那么主电源供电的网关更可靠，并能够防御外部攻击。

攻击也可以根据攻击者的能力进行分类，如发生在传感器层或计算机层。强大的计算机层攻击对 WSN 的破坏比恶意的传感器节点的破坏大得多，因为与电池驱动的传感器节点相比，它有更强大的电源、计算能力和通信能力。WSN 面临的更频繁的攻击是根据网络的层次分类的。这种分类是根据攻击事件是发生在物理层、链路层、网络层、传输层或应用层来划分的。Wood 和 Stankovic（2002）把 WSN 面临的各种 DoS 攻击根据网络的层次分类，并通过一个表列出了典型传感器网络的层次，描述了每层的漏洞和防御。每层对不同类型的 DoS 攻击都有弱点，可以有不同的防御选择。一些攻击可穿越多层，或者利用层间的交互。Du 和 Chen（2008）总结了传感器网络的典型攻击和可能的防御技术。表 9.2 给出了传感器网络层次和 DoS 防御技术。

表 9.2 中，当所有要素，如干扰、篡改、冲突、耗尽、不公平、忽略和贪婪、自动引导、汇聚口、洪泛、去同步可以归类为 DoS 攻击，因为这些手段减弱或消除了网络执行预期功能的能力。密钥管理是任何安全服务的重要内容。下一节将介绍基于 ZigBee 的 WSN 的密钥管理。然后，为了限制篇幅，本章的剩下部分将重点介绍外部 DoS 攻击及 WSN 的室内应用。

表9.2 传感器网络层次和DoS防御技术

网络层次	攻击	防御技术
物理层	干扰	扩频、优先信息、低占空比、区域映射、模式改变
	篡改	防篡改、隐藏
链路层	冲突	纠错编码
	耗尽	速率限制
	不公平	短帧
网络层	忽略与贪婪	冗余、探测
	操纵路由信息	认证、加密
	女巫攻击	认证
	虫洞攻击	监视、灵活路由选择
	选择转发攻击	冗余、探测
	自动引导	加密
	误导	出口过滤、授权、监视
	汇聚口	授权、监视、冗余
运输层	洪泛	有限连接，客户迷惑
	去同步	认证
应用层	克隆攻击	唯一的成对密钥

9.4 ZigBee 安全防御服务

ZigBee 安全防御服务所提供的方法包括，密钥构建、密钥传输、帧保护和设备管理。其服务分为两种模式：一种是 ZigBee 和 ZigBee PRO 使用的标准模式；另一种是 ZigBee PRO 使用的高级安全模式。ZigBee 安全服务设计要遵循的原则是由生成帧的层负责帧的初始化安全。例如，如果一个网络层命令帧需要保护，则需要使用网络层的安全服务。ZigBee 使用计数器加密（Counter Mode，CTR）、密文分组链接（Cipher Block Chaining，CBC）、消息完整码（Message Integrity Code，MIC）及128位高级加密标准（Advanced Encryption Standard，AES）算法（Elahi 和 Gschwender，2009）。

9.4.1 用于 ZigBee 安全防御的密码学

密码学是对信息进行加解密来保证信息安全的一种技术，通常包括加密和解

密。原文是指没有加密的明文，而把加密的信息称为密文。明文采用某种加密算法和加密密钥进行加密；然后在信道里传送密文；最后，在接收端使用解密密钥和解密算法进行解密。图 9.1 给出了加解密过程。



图 9.1　加解密过程

有两种加密技术：一种是对称密钥加密技术，另一种是非对称密钥加密技术。在对称密钥加密技术中，消息的发送者和接收者使用相同的密钥分别对信息进行加密和解密。与对称密钥加密技术不同，在非对称密钥加密技术中信息的发送者和接收者分别使用不同的密钥进行加密和解密。密码块是指被同时加密的一组二进制数据，流密码是指一位接一位加密的二进制数据。

9.4.1.1　高级加密标准

高级加密标准（Advanced Encryption Standard，AES）是一种块加密技术，它使用 128 位、192 位或 256 位的密钥加密数据块。基于 ZigBee 的安全防御采用的是 128 位的密钥（4×4 的字节数组，即 4×4×8bit = 128bit）。图 9.2 给出了 128 位密钥和密文状态。

$K_{0,0}$	$K_{0,1}$	$K_{0,2}$	$K_{0,3}$
$K_{1,0}$	$K_{1,1}$	$K_{1,2}$	$K_{1,3}$
$K_{2,0}$	$K_{2,1}$	$K_{2,2}$	$K_{2,3}$
$K_{3,0}$	$K_{3,1}$	$K_{3,2}$	$K_{3,3}$

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

图 9.2　128 位密钥和密文状态

AES 的加密过程包括 4 步：替代、行移位、混列和添加轮密钥，如图 9.3 所示。这个过程重复 10 次完成一次加密过程。

第 1 步，根据转换表（也称作 S-Box 表），用另一个字节替代加密状态中每个字节。

第 2 步，将第一步产生的状态矩阵的每一行使用下面的操作完成行移位（见图 9.4）：

- 第 1 行不移位；
- 第 2 行循环左移 1 位；
- 第 3 行循环左移 2 位；

● 第 4 行循环左移 3 位。

第 3 步，将给定的常量矩阵乘上第 2 步产生的结果矩阵，如图 9.5 所示。

第 4 步，将第 3 步的结果矩阵与 128 位的密钥矩阵进行异或操作，如图 9.6 所示。

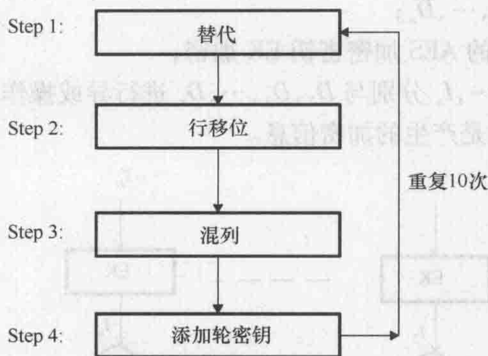


图 9.3　AES 加密过程

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,1}$	$S_{1,2}$	$S_{1,3}$	$S_{1,0}$
$S_{2,2}$	$S_{2,3}$	$S_{2,0}$	$S_{2,1}$
$S_{3,3}$	$S_{3,0}$	$S_{3,1}$	$S_{3,2}$

图 9.4　行移位操作

$$\begin{vmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{vmatrix} \times \begin{vmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,1} & S_{1,2} & S_{1,3} & S_{1,0} \\ S_{2,2} & S_{2,3} & S_{2,0} & S_{2,1} \\ S_{3,3} & S_{3,0} & S_{3,1} & S_{3,2} \end{vmatrix} = \begin{vmatrix} A_{0,0} & A_{0,1} & A_{0,2} & A_{0,3} \\ A_{1,0} & A_{1,1} & A_{1,2} & A_{1,3} \\ A_{2,0} & A_{2,1} & A_{2,2} & A_{2,3} \\ A_{3,0} & A_{3,1} & A_{3,2} & A_{3,3} \end{vmatrix}$$

图 9.5　混列操作

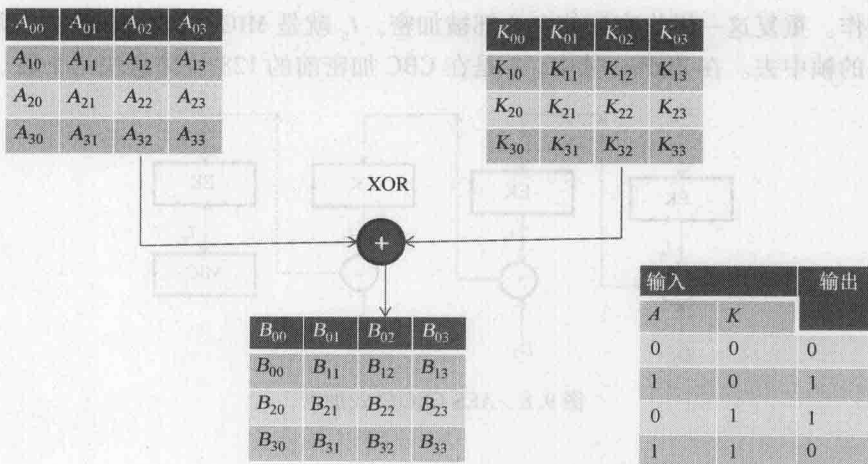


图 9.6　异或操作

9.4.1.2　计数器模式加密

计数器模式由如下操作来完成（见图 9.7）:

T_1 是一个计数值，$T_2 = T_1 + 1, T_3 = T_2 + 1, \cdots, T_n = T_{n-1} + 1$。EK 是 128 位的 AES 加密密钥。

- 将信息分割成信息块 $D_1, D_2, \cdots, D_n$；
- 将 $T_1, T_2, \cdots, T_n$ 采用 128 位的 AES 加密密钥 EK 加密；
- 将上一步产生的结果 $I_1, I_2, \cdots, I_n$ 分别与 $D_1, D_2, \cdots, D_n$ 进行异或操作；
- 输出的结果 $P_1, P_2, \cdots, P_n$ 就是产生的加密信息。

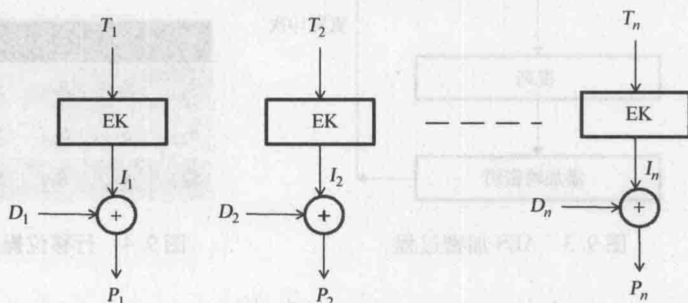


图 9.7　AES 计数模式加密

9.4.1.3　密文分组链接模式加密

CBC 模式加密在 ZigBee 安全服务中被用来生成信息完整码（Message Integrity Code，MIC）以维护数据的一致性。如图 9.8 所示，将信息分割成 128 位的信息块。第 1 块 D_1 采用 128 位的 AES 密钥加密，产生的密文 I_1 与下一块信息 D_2 进行异或操作。重复这一操作直到信息全部被加密。I_n 就是 MIC，在必要时将其添加到 ZigBee 的帧中去。在 ZigBee 帧中，n 是在 CBC 加密前的 128 位信息块的个数。

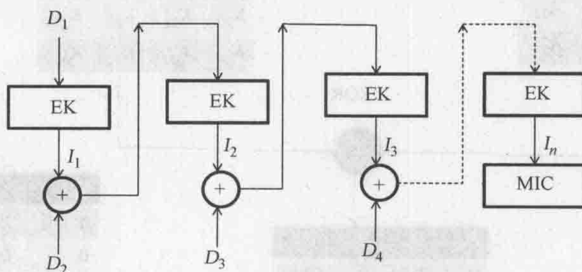


图 9.8　AES CBC 模式加密

9.4.2　ZigBee 安全密钥和信任中心

ZigBee 的 WSN 的安全是基于一些“链接”密钥、网络密钥和主密钥。ZigBee 信任中心，也叫做安全服务提供者，负责管理网络安全和密钥分配。ZigBee 信任中

心在 ZigBee 协议栈中位于网络层和应用支持子层，如图 9.9 所示。

● 链接密钥。链接密钥是应用协议子层用来确保 ZigBee 设备之间单播通信的安全的，有以下两种类型的链接密钥：

-应用链接密钥。这种链接密钥用来确保两个设备之间应用数据的安全，并且它只在两个设备间共享。设备通过密钥传输、密钥建立或预安装的方式获取链接密钥。

-信任中心链接密钥。这种密钥是信任中心和网络设备用来确保信任中心与设备之间的通信安全的。这种密钥是在设备中预先配置好的。

● 网络密钥。网络密钥是在网络层的广播通信中使用的。网络中的所有设备共享相同的网络密钥，因为所有设备必须能够解密这些网络广播信息。这种密钥被设备制造商安装到设备上或通过信任中心传输给设备的。

● 主密钥。主密钥用于生成链接密钥。这种密钥可以由信任中心制造商预先安装。

● 信任中心。信任中心是在网络中所有设备都信任的设备，负责分配网络密钥和端到端应用配置管理。网络中的所有成员都将准确地识别一个信任中心，而且在每一个安全网络中只有一个信任中心。ZigBee 规范中定义了信任中心应承担的角色。其角色可分为三个子角色：信任管理者、网络管理者和配置管理者。一个设备通过信任它的信任管理者来识别设备的网络角色和配置管理者。网络管理者负责分配网络密钥给相应的网络设备，并维护和管理网络密钥。配置管理者负责绑定两端的应用，并使其在管理的设备间建立端到端的安全通信（如通过分配主密钥和链接密钥）。为了简化信任管理，这三个子角色可以包含在一个单独的设备上——信任中心。（ZigBee Alliance，2005）

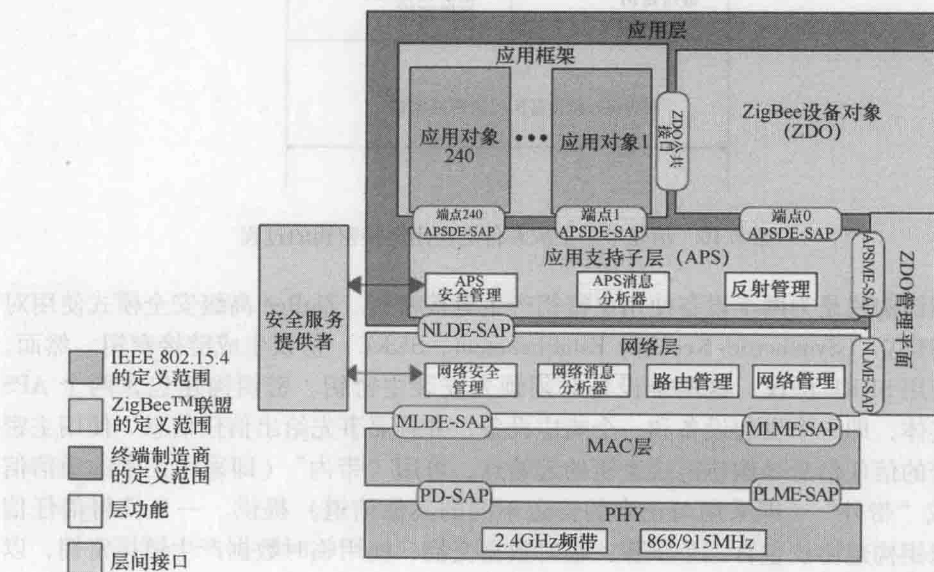


图 9.9 ZigBee 协议栈

9.4.3 密钥传输与密钥构建

密钥的传输可以在安全模式或非安全模式下进行。在安全密钥传输模式下，信任中心负责将链接密钥、网络密钥和主密钥传输给各种设备。在非安全模式下，密钥随着设备进行加载。在安全密钥传输模式下，信任中心执行下述功能。

● 网络密钥传输

WSN 的信任中心和设备采用预先配置好的信任中心链接密钥从信任中心向设备传送新的或活跃的网络密钥，过程如下：

- 当一个新设备加入 WSN 时，信任中心加密一个活跃的网络密钥并将其传输给该设备；

- 如果某个设备请求网络密钥更新，信任中心使用信任中心链接密钥加密一个新的网络密钥并将其发送给该设备。

● 应用链接密钥传输

在接收到设备的请求后，信任中心生成应用链接密钥确保两个设备之间的应用数据的安全通信。信任中心采用预配置的信任中心链接密钥对产生的应用链接密钥进行加密，然后将其传输给设备。信任中心生成和传送应用链接密钥的过程如图 9.10 所示。

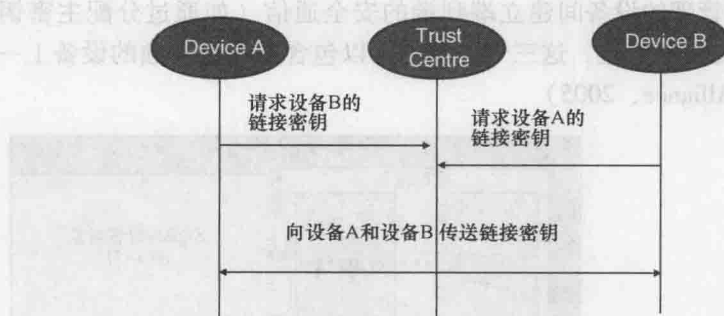


图 9.10 信任中心生成和传送应用链接密钥的过程

密钥构建是为两个设备使用主密钥产生链接密钥。ZigBee 高级安全模式使用对称密钥建立（Symmetric-Key Key Establishment，SKKE）协议生成链接密钥。然而，为了使用 SKKE 协议，这两个设备必须预先安装主密钥。密钥构建包含两个 APS 管理实体，即一个发起设备和一个响应设备，并且要事先给出信任信息。使用主密钥加密的信任信息是构建链接密钥的起始点，可用“带内”（即采用正常的通信信道）或“带外”（即采用与正常的信道不同的其他信道）提供。一旦获得信任信息，密钥构建协议包含三个步骤：临时数据交换，使用临时数据产生链接密钥，以及确认链接密钥的正确性。

9.5 防御拒绝服务攻击的典型策略

有大量的方法保护资源丰富的服务器和网关免受DoS攻击（Ricciato等，2010）。这些方法可以分为基于受害方的方法、基于攻击方的方法和基于防御方法的位置的混合方法（Mirkovic，2003）。基于受害方的防御方法从受害方的角度通过资源倍增（Chiba等，2006）或将受害方的连接缓冲区迁移到系统资源更大的设备上建立连接的方式（Schuba等，1997）来降低影响和处理DoS攻击。然而，所有服务器仍然要面对被更大的DoS攻击耗尽资源的风险。基于攻击方的防御方法则是从攻击方的角度来保护受害方不受攻击的方法。这类方法中的典型例子有在线包统计的多级树方法（Multi-Level Tree for Online Packet Statistics，MULTOPS）（Thomer和Massimiliano，2001）、DoS网络攻击识别与防御（DoS netWork Attack Recognition and Defence，D-WARD）（Mirkovic等，2003）、特定消息迷惑方法（Ning等，2008），以及可扩展广播认证方案X-TESLA（Kwon和Hong，2010）等方法。例如，运行在私有网络和因特网之间的路由器上的D-WARD是用来防止私有网络的主机发送DoS攻击数据包。D-WARD方法分析到达的通信量，并通过“无响应主机”检测技术来检测DoS攻击。“无响应主机”发送的所有数据包都发送至某个IP地址。此外，入口过滤方法用来确保所有出口的数据包拥有有效的子网地址以避免IP欺骗。混合预防方法从受害方和攻击方两方面处理攻击，如聚集拥塞控制（Aggregate Congestion Control，ACC）（Ratul等，2002）。

采用两个理论方法来分析上面的DoS防御方法的细节。第一步，现有的DoS防御方法检测DoS攻击开始的时间和试图区别合法的网络通信量和来自DoS攻击的网络数据。第二步，现有方法试图转移任何检测到的DoS攻击。处理DoS攻击的主要困难是如何区分合法的网络数据和来自DoS攻击的网络数据。因此，有一定比例的DoS攻击数据被误认为是合法的网络数据而允许其到达受害方设备，如现有方法不能有效地过滤掉所有的DoS攻击数据。典型的DoS防御方法的比较见表9.3，表中给出了三种普遍应用的DoS防御方法的有效性（Mirkovic，2003；Thomer和Massimiliano，2001；Ratul等，2002）。从表9.3可以看出，D-WARD是最有效的DoS防御方法，可以过滤掉99.4%的DoS攻击数据。然而，它仍无法避免少量误判的深攻击通信量到达受害方设备。

在相对资源丰富的计算机的DoS攻击防御中，现有的DoS防御方法达到了一个令人满意的保护水平。少量的DoS攻击不足以使合法用户的服务崩溃。然而，DoS深攻击目标是传感器网络和因特网之间的入口点（这个点叫做网关），它将足以阻止远程用户与WSN的通信。并且，一旦DoS深攻击数

据穿过网关，它将足以淹没传感器网络有限的带宽资源并迅速耗尽无线传感器中间节点的稀缺的不可再生的电源。本章余下的内容将设计、实现和测评基于第三方的针对 WSN 的 DoS 深攻击转移方法。该方法与现有的 DoS 计数器测量方法一起完成 DoS 深攻击转移。下面将采用基于 WSN 的智能家居系统为例加以讨论。

9.6 基于无线传感器网络的智能家居系统拒绝服务深攻击的防御

智能家居系统（Home Automation System，HAS）是为提升居民生活品质而引入家居中的技术，它可提供如远程医疗、多媒体娱乐和节能等不同的服务。智能家居系统也能检测和控制家用器具，用户能舒适而有效地管理家居。在研究和工业领域，近期的发展趋势是开发基于 WSN 的 HAS。目前，拥有丰富资源的防御 DoS 攻击的方法可以消除绝大部分攻击流量。然而，基于 WSN 的 HAS 因为资源有限对 DoS 深攻击的防范还是很脆弱的。

本节介绍一种防御设计，可以完善现有的 DoS 防御方法，并对资源有限的基于 WSN 的 HAS 的保护进行改进以免受 DoS 深攻击。DoS 攻击方法由三个实体组成：“虚拟家居（Virtual Home，VH）”，“远程家居服务器（Remote Home Server，RHS）”，“DoS 防御服务器（DoS Defence Server，DDS）”，如图 9.11 所示。包括攻击者在内远程用户和 HAS 之间有两种连接方法。图 9.11 所示的①和②方法称作 RHS-1，所示的③方法称作 RHS-2。RHS-1 是一个加密的第三方连接，而 RHS-2 是一个加密的直接连接。不区分的 DoS 深攻击通过安全信道到达测试设备的流量情况见表 9.3。虚拟家居的主要目标是侦测和过滤任何到达的 DoS 攻击，阻止它们到达真正的 HAS。此外，在任何 DoS 攻击的过程中，虚拟家居还负责保证与远程用户进行有效通信。虚拟家居包含了 DoS 攻击检测机制和 DoS 攻击转移机制。RHS 被设计成资源丰富的可信任的第三方，用于 DoS 攻击发生时构建一个中间通信信道。DoS 防御服务器驻留于 RHS，为 HAS 提供时延分析。

表 9.3 典型的 DoS 防御工具的比较

DoS 防御工具	DoS 攻击数据包移除的比例
D-WARD	99.4
ACC	64
MULTOPS	93

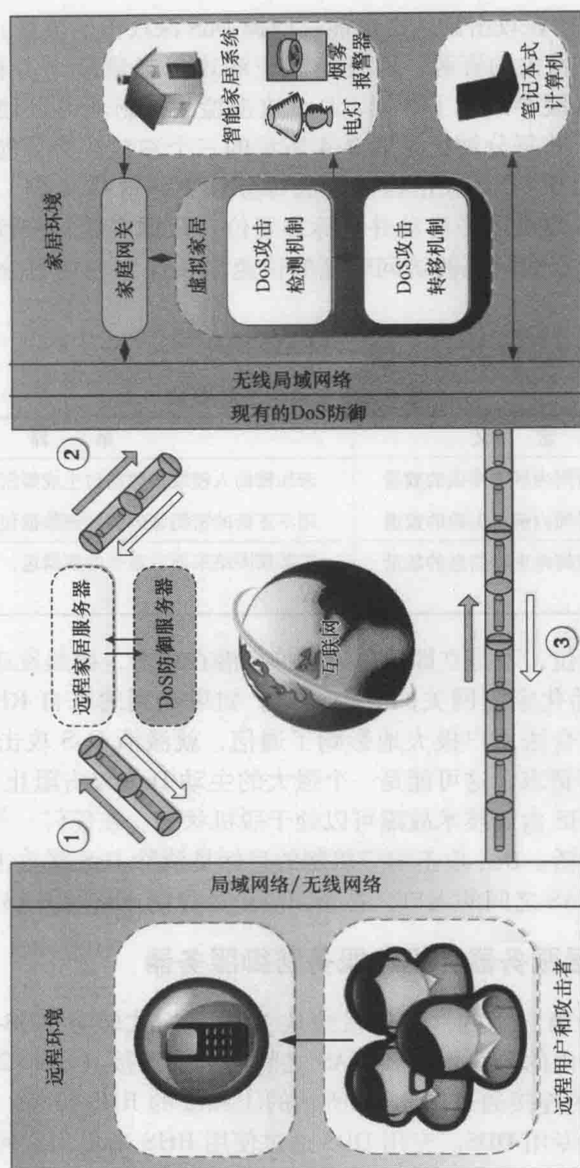


图 9.11 基于 WSN 的 HAS 针对 DoS 深攻击防御的虚拟家居方法

9.6.1 虚拟家居：拒绝服务攻击监视和防御触发

如图 9.11 所示，系统使用的远程通信架构加密了远程用户和 HAS 之间的所有通信。端到端的加密用来保护用户的隐私免受恶意用户的攻击。这样做的好处是，就 DoS 攻击防御而言，所有的入侵攻击 100% 能够被检测到，除非攻击者拥有加密

的密钥。这使得 VH 在攻击到达之前能过滤掉 DoS 深攻击的流量。这不仅能阻止深攻击流量耗尽家庭网关的资源，而且能阻止深攻击流量最终占有全部的 WSN 带宽。一旦系统输入缓存出现了数据，DoS 攻击检测机制就可以侦测到加密的和非加密的入侵数据，并每分钟记录表 9.4 所示的三个参数。为了简单起见，这些参数的初始值均设为 0。DoS 攻击检测算法每分钟更新这些参数。如果满足下面的规则，就认为 DoS 攻击已经启动并将标志置位。根据实验，将预定义的阈值设定为 300。实验表明家庭网关的访问时延的快速增长仅出现在每分钟的攻击数量超过阈值之后。

规则：If（DE + DF + RM）>300：FLAG

表 9.4 主要的系统参数

参数	定义	解释
DE	给定时间内解密错误的数量	未加密的入侵攻击数据包生成解密错误
DF	给定时间内解密失败的数量	用不正确的密钥编码的加密数据包成功解码失败
RM	给定时间内重播信息的数量	在某期限结束前后重播的数据包，不能解密或生成新的错误

一旦标志被置位，不是立即采取措施抑制潜在攻击，而是发送一个消息至下面描述的 RHS 去初始化家庭网关的分析模块。如果收到的来自 RHS 的分析结果表明，一个攻击通过合法用户极大地影响了通信，就激活 DoS 攻击响应机制。如果 RHS 不能响应分析请求，这可能是一个强大的主动 DoS 攻击阻止了 RHS 与家庭网关通信。此外，RHS 由于技术故障可以处于脱机状态。在任何一种情况下，DoS 攻击响应机制都被激活。DoS 攻击响应机制的目标是消除 DoS 深攻击。DoS 深攻击的目标为因特网和 HAS 之间的入口，并企图阻止远程用户访问 HAS。

9.6.2 远程家居服务器和拒绝服务防御服务器

RHS 被设计为第三方的。一旦系统从 RHS-2 模式转至 RHS-1 模式，也就是说，包括攻击者在内的合法用户和 HAS 之间的直接连接（RHS-2）失效时，合法用户和 HAS 之间的连接通过图 9.11 所示的①和②的 RHS 维持。RHS 收到的 DoS 分析请求被路由到专用 DDS。专用 DDS 通过使用 RHS 来阻止任何对合法用户服务的影响，其中使用 RHS 是为了通信的需要。DDS 的作用是模拟一个希望远程访问 HAS 的合法智能家居的用户，以及计算平均连接时延。DDS 计算从模拟的移动设备重复连接到 HAS 的相关家庭网关的时延，并作为服务下降的值。对企图进行的十次连接求平均时延，如果服务下降超过了预先由各自用户设定的阈值，那么就向各自的 VH 发送消息来转移攻击；否则，信息被发送至 VH 并不采取行动。

9.6.3 虚拟家居：拒绝服务攻击转移机制

DoS 攻击响应机制的目的是，通过对 DDS 执行的连接时延分析来转移检测到

的 DoS 攻击，并维护远程用户和 HAS 之间的有效通信，消除针对家庭网关的任何低速率 DoS 攻击。正如前文的描述，DoS 攻击响应机制使用两个连接方法：RHS-1 和 RHS-2。RHS-2 在正常条件下使用，在远程用户和 HAS 之间直接建立一条安全连接，即图 9.11 所示的③。这种连接方法提供了最佳的通信性能。RHS-1 常用于 DoS 攻击状态下，并通过一个资源丰富的可信任的第三方在远程用户和 HAS 之间建立一个间接安全连接。这个第三方可表示为 RHS，即图 9.11 所示的①和②。DoS 攻击转移机制是在 DoS 攻击的条件下，将 RHS-2 连接方法切换为 RHS-1 连接方法。一个来自 DoS 防御服务器的消息触发了 VH 系统从而使所有支持到 HAS 的访问连接失效，并创建一个到 RHS 的出口连接。连接到 RHS 的远程用户在远程用户和 HAS 之间创建了一个安全信道。研究表明，RHS-1 方法比 RHS-2 方法慢 93%（Gill 和 Yang，2008）。然而，在 DoS 攻击期间，使所有入连接失效的 DoS 攻击转移机制的效果，是终止所有 DoS 攻击的入连接。只有合法用户能转换至 RHS-1 连接方式，并拥有 RHS 授权，建立与 HAS 的间接安全连接。所有到智能家居网络的通信一定遍历从 HAS 至 RHS 的出口连接。任何进一步的从攻击者到 HAS 的直接连接请求立即被丢弃，并且从基于 WSN 的 HAS 中移除攻击焦点和瓶颈。所以，攻击者不得不针对相对资源丰富的可信任的 RHS 发起一个更强的 DoS 攻击。

当用户定义的时间段结束或 DoS 攻击结束，DoS 攻击转移机制切换回 RHS-2 方式。如果 DoS 攻击没有结束，那么系统维持在 RHS-1 通信方式下。周期性地执行 DoS 攻击检测以确定 DoS 攻击结束和 RHS-1 方式重新开始的时间。假如家庭网关不能建立一个到 RHS（RHS-1 模式）的连接，就假定 RHS 出现技术故障，并启动 RHS-2 通信模式。

9.6.4　虚拟家居的实现

如 9.6 节开头所提到的，现有的用于处理 DoS 攻击的系统主要位于测试目标网络的边缘。近来提出的新系统分散地分布在因特网内或者位于测试目标网络的边缘。这些方法采用全权委托的方法过滤网络流量。现有的方法设计成过滤所有通过两点之间的因特网流量。如图 9.11 所示，VH 位于智能家居网络的边缘，安装在家庭网关上，位于智能家居网络边缘和提供访问因特网的家居局域网之间。家庭网关在其他网络和智能家居网络间起到关键的桥接作用。所有的进或出智能家居的数据都要经过这个连接。VH 的位置允许精确地检测和过滤智能家居的数据，同时允许到其他网络的数据由现有的 DoS 防御进行检测或不检测。如图 9.11 所示，笔记本式计算机用户能直接连接到因特网，与 VH 没有关系。该方法允许对所有智能家居通信进行加密，而加密的优势是为了防止 DoS 攻击，正如前面所提到的。同时，该方法节省了可观的用于处理和猜测来自正常数据的攻击数据的计算资源，这些数据位于因特网和家居局域网之间的访问入口的局部网络边缘。

VH 的实现就要允许加密所有智能家居的通信，为智能家居系统提供完全的保

护。除非家居密钥被攻击者获得，否则攻击流量不会通过基于受约束的 WSN 的 HAS 被发送。VH 的伪代码见表 9.5。

表 9.5 VH 的伪代码

步骤 1：在应用是活动的整个时间内，每分钟调用函数来分析解密结果

```
Timer(60000);
Function Timer(Delay){
        analysis();
        Timer(60000);
}
```

步骤 2：当系统输入缓存一有数据就调用解密函数，在这个过程中记录所有的重放、解密失败和解密错误信息

```
Function decrypt(){
        rawMessage = (inputBuffer);
        message = decrypt(rawMessage);
        if(message.nonce not correctly incremented){
                nonceReplay = nonceReplay + 1;
        } else if(message.decryption = fail){
                decryptionFailure = decryptionFailure + 1;
        }else if(message.decryption = error){
                decryptionError = decryptionError + 1;
        }else if(message.DDSAnalysisResult){
                switch(message.DDSAnalysisResult);
        }
}
```

步骤 3：这个函数每 60 000ms 被执行一次；如果潜在的 DoS 攻击被侦测到，就发送消息到 DDS，执行基于 WSN 的 HAS 连接时延分析

```
Function analysis(){
        int Flag = 0;
        if(nonceReplay > 0){
                Flag = 1;
                nonceReplay = 0;
        }if(decryptionFailure > 0){
                Flag = 1;
                decryptionFailure = 0;
        }if(decryptionError > 0){
                Flag = 1;
                decryptionError = 0;
        }if(Flag == 1){
                Send(WSN based HAS analysis request to DDS);
        }
}
```

（续）

步骤4：这个函数选择基于 WSN 的 HAS 正在使用的通信方法

```
Function Switch(message.DDSAnalysisResult){
            if(message.DDSAnalysisResult equals “switch”){
                        Switch to using the third party RHS-1 Approach(); //Stop support
   for incoming connections
            }else if (message.DDSAnalysisResult equals “do not switch”){
                        Do not switch communications approach(); //Continue using
   direct RHS-2 approach
            }
}
```

9.7 利用虚拟家居防御拒绝服务对智能家居的攻击的实现

本节描述了9.6节讨论的 DoS 深攻击防御方法的实现，介绍了发起 DoS 深攻击的攻击工具开发情况，并对基于 VH 的防御方法进行了测试。RHS 系统架构如图9.12所示，DoS 防御策略由四部分组成。

首先，安装在移动手机的 RHS 客户端向用户提供了图形用户界面，并处理和 HAS 的连接。其次，安装于资源丰富的可信任的第三方的 RHS，是 RHS-1 和 RHS-2通信方式的主要部分。第三，DDS 驻留在 RHS 里，提供 HAS 连接时延的分析。第四，主要驻留 VH 的家庭网关，提供 DoS 侦测和转移机制。

9.7.1 远程家居客户端

RHS 客户端是在一个标准移动电话（如 J2ME midlet）上实现的。midlet 为 HAS 提供 TCP 连接和用户界面。安全功能是通过集成免费资源 Bouncy Castle API 和 midlet 实现的。使用 Bouncy Castle API 允许利用完善和已测试安全的 API。

9.7.2 远程家居服务器

RHS 是在标准的笔记本式计算机上实施的。RHS 在 C#中编码，使用 .NET 框架2.0。尽管 .NET 框架自己提供了安全库，但是由于 HAS 的资源限制，正如后面将要讨论的，.NET 框架库因不能提供所需的加密算法而无法使用。因此，Bouncy Castle API 的 C#实现用来提供需要的安全功能。RHS 的一个关键部分是 RHS 数据库服务器。数据库维护所有互联家居的信息。数据库是使用 Microsoft SQL server 2005 实现的。

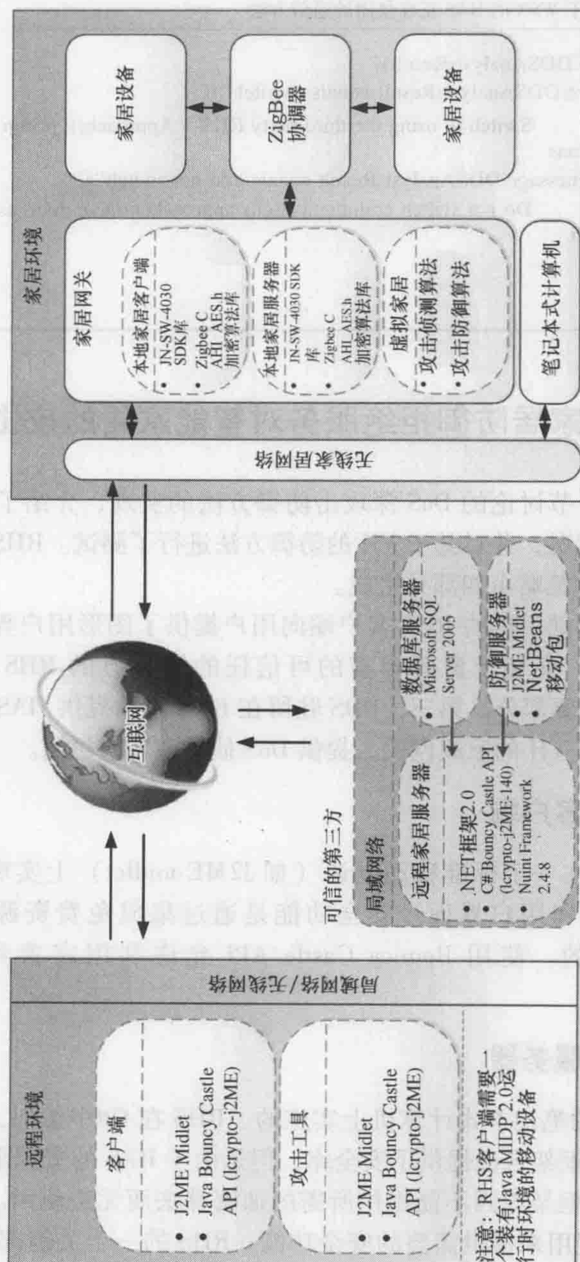


图9.12　RHS系统架构

9.7.3　拒绝服务防御服务器

一个标准的笔记本式计算机包含了 DDS。DDS 由 Java midlet 和仿真移动电话组成。NetBeans 移动包 5.5 被用来模拟运行 Java midlet 的移动电话。Java midlet 试图初始化预定义的到家庭网关的连接数量，并计算平均连接时延。此外，midlet 创建了一个到 RHS 的 TCP 连接来表明各自的 HAS 的平均连接时延。DDS 的伪代码见表 9.6。

表 9.6　DoS 防御服务器伪代码

步骤 1：调用函数分析各自的家居连接延迟

```
Function latencyCheck(){
        long averagelatency = 0;
        long sumLatency = 0;
        int NumberofChecks = 50;
        int counter = 0;
```

步骤 2：通过连接到各个基于 WSN 的 HAS，总计连接延迟时间仿真一个移动用户

```
  connection latency
        while(counter < NumberofChecks){
                Thread.sleep(1,000); //adds a 1,000 ms delay between connection
  attempts
                long startTest = System.currentTimeMillis();
                long endTest = send(message); //The send message returns the system
  time when the
                                                                //send completes,
  including connection times.
                        sumLatency = sumLatency + (endTest-startTest);
                        counter++
}
```

步骤 3：计算平均连接延迟，并与预定义的延迟阈值进行比较，通知基于 WSN 的 HAS 计算结果

```
        averageLatency = (sumLatecy/NumberofChecks);
    If(averageLatency ≥ 3,000){
                Send(switch message to WSN based HAS);
        }else{
                Send(latency below threshold message to WSN based HAS);
        }
}
```

9.7.4　家居网关

2009 年 Gill 等人开发了低成本、主电源供电的独立的家庭网关。独立网关在因特网和基于 WSN 的 HAS 之间提供路由，其中基于 WSN 的 HAS 与 IEEE 802.11g

兼容的局域网进行桥接。家庭网关集成了一个 JN5139 ZigBee 无线通信模块（图 9.13 所示的左上角具有天线的器件）和一个 WiMe web 服务器（图 9.13 所示的右上角具有天线的器件）。在基于 WSN 的 HAS 中，充当路由器的家庭网关可以与 ZigBee 协调器或通信范围内的其他路由器进行通信。这可以在资源有限的 HAS 上对所提出的 DoS 防范策略进行测评。

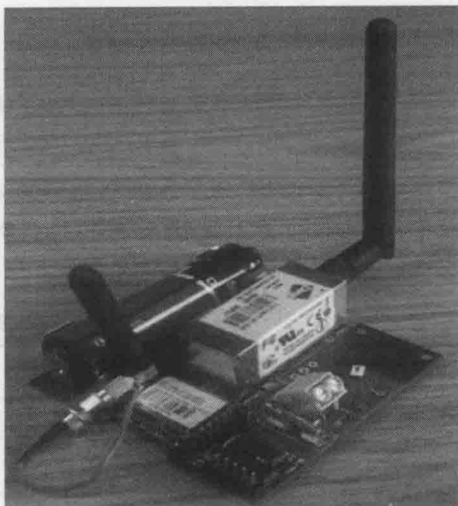


图 9.13　家庭网关

家庭网关负责与本地家居客户端、家居服务器和 VH 的通信。家庭网关应用在一个 ZigBee 微处理器上实现。微处理器使用 ZigBee AHI-AES. h 库提供需要的安全功能。由于资源限制，加密算法和操作模式都受到了限制。从可用的选择中，选择了先进加密标准（Advanced Encryption Standard，AES）加密算法，该算法在具有 CBC-MAC 的计数器（Counter with CBC-MAC，CCM）模式下操作。CCM 是块密码模式，可以提供信息的保密性和完整性。由于存储器空间的限制，不能分别实现加密和完整性检查算法。此外，AES CCM 分别由 J2ME 的 Bouncy Castle API 以及用于移动客户端和 RHS 的 C#程序提供支持。

家庭网关负责在通信模式 RHS-1 和 RHS-2 之间进行切换。家庭网关可以启动和停止到达的 TCP 连接服务，以及对预定义的 IP 地址构建 TCP 出连接。家庭网络不接受 UDP 连接，因为像基于 WSN 的 HAS 这样的资源有限的网络不需要 UDP 连接。

9.8　测评

DoS 深攻击的防御方法的测评是在一个真实的家居环境里实施的。测评由两个步骤组成：首先，通过攻破 D-WARD 这个现有防御方法，研究了 DoS 深攻击对基于 WSN 的 HAS 造成的破坏；其次，研究了这里提出的方法对保护家庭网关免受 DoS 深攻击方法的有效性。

9.8.1　攻击工具

为了发起对家庭网关和相关 HAS 的 DoS 深攻击来验证对基于 WSN 的 HAS 攻击的有效性及测评该方法的效果，这里开发了一个攻击工具。

为了测试深攻击对用现有 DoS 防御方法保护基于 WSN 的 HAS 的有效性，攻击

工具向家庭网关发送非加密数据，随后将其通过 WSN 转发至测试设备。此外，攻击工具启功一个针对 WSN 应用层的 TCP 攻击，以便验证所提出的方法对保护基于 WSN 的 HAS 免受攻击的有效性。该攻击以家庭网络为目标，并企图阻止远程用户有效地访问系统。攻击工具基于这样的事实，家庭网关允许临时构建 TCP 连接接收验证数据。如果连接在初始化后一直保持空闲并且家庭网关没有收到验证数据，那么家庭网关就拒绝该连接。然而，攻击工具试图通过初始化 TCP 连接和对合法数据、带有随机密钥的加密数据和非加密数据的信息重放的发送来耗尽家庭网关的连接验证机制。在拆除活动连接之前，家庭网关不得不鉴别验证信息的有效性。由于家庭网关资源受限的特性，当家庭网关正验证大量的连接时，合法用户可能无法获得连接。Bouncy Castle API 为攻击工具提供了必要的加密功能来启功攻击。攻击工具的伪代码见表 9.7。

表 9.7　攻击工具的伪代码

1：调用攻击函数开始攻击

```
Function Attack (String attackType)
{
```

2：根据请求的攻击类型，生成和初始化攻击数据

```
String attackMessage = "";
        If(attackType == "UnencryptedDataAttack"){
                attackMessage = UnencryptedDATA;
        }
        If(attackType == "IncorrectlyEncryptedDataAttack"){
                attackMessage = IncorrectlyEncryptedData;
        }
        If(attackType == "CapturedDataReplayAttack"){
                attackMessage = ReplayedEncryptedData;
        }
```

3：开始攻击直至攻击者决定停止攻击

```
        Boolean attackStatus = true;
        while (attackStatus) {
                Open connection to victim (IP Address, Port)
                Send(attackMessage);
                Close connection to victim(IP Address, Port)
                If(stopAttack){
                        attackStatus = false;
                }
        }
}
```

9.8.2 基于无线传感器网络智能家居的拒绝服务深攻击的分析

基于 WSN 的 HAS 通过家庭网关与一个本地无线 Wi-Fi 网络连接。一个本地笔记本式计算机也连接至本地无线 Wi-Fi 网络中。基于 WSN 的 HAS 转变成一个星形拓扑结构，其中 ZigBee 协调器位于家庭环境的逻辑中心，如图 9.12 所示。上面讨论的攻击工具发送的攻击数据经因特网穿过本地无线 Wi-Fi 网络到达基于 WSN 的 HAS，然后再到家庭网络，最后到达测试设备。这个测试设备是个 ZigBee 协调器。仿真中，在攻击流量到达家庭网关之前，D-WARD 攻击防御工具在本地 Wi-Fi 网络阻止了 99.4% 的攻击流量，而只有 0.6% 的攻击数据攻破家庭网关到达测试的 ZigBee 协调器。如图 9.14 所示，在实验开始时，没有攻击数据发送至基于 WSN 的 HAS，本地笔记本式计算机和测试的 ZigBee 协调器之间的正常通信的丢包率的测量值为 2.5%。接着，增加攻击率，对于每个攻击率都重复进行 10 次实验，并计算平均丢包率。从实验中可以发现，攻击率小于 32packet/min[⊖] 造成的丢包率和正常的丢包率几乎没有区别。但是，当攻击增加到 50packet/min 时，本地笔记本式计算机和测试的 ZigBee 协调器之间平均丢包率约为 26.9%。由于进一步增加了攻击率，所以丢包率也随之增加。当攻击率为 128packet/min 时，有 73.5% 的数据包丢失。当攻击率增加到 256packet/min 时，丢包率上升到 86.25%。

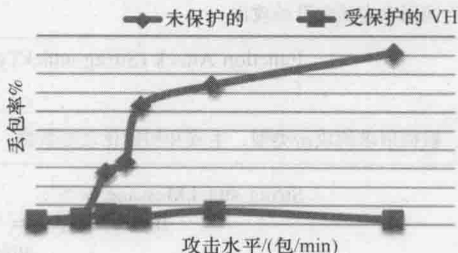


图 9.14 在基于星形拓扑的 Zigbee 网络中不同 DoS 攻击水平下的平均丢包率

用本章提出的 DoS 防御方法在家庭网关中重复上述实验。如图 9.14 所示，VH 有效阻止了攻击数据经家庭网关到达测试的 ZigBee 协调器；另外，在远程 DoS 深攻击期间，本地计算机和试验用 ZigBee 协调器之间通信的丢包率没有显著的不同，平均丢包率在 1.9% ~6%。

攻击时，数据包长度为 133B。基于 ZigBee 的 WSN 的最大带宽为 31.25KB/s，即 250kbit/s（ZigBee Alliance，2005）。上面的实验表明，(256 ÷ 60 × 133) B/s = 567B/s 的攻击会使 86.25% 的数据包丢失。在这个实验中，攻击通信量只占 ZigBee 带宽的 1.8%。若要 567B/s 的通信量绕过 D-DWARD 防御系统并到达测试的 ZigBee 协调器，则攻击端的攻击通信量为（567 ÷ 0.6% ÷ 1000）kB/s = 94.5kB/s。由此可以知道，小规模的 DoS 深攻击（94.5kB/s）和小比例的带宽占用都会对基于 ZigBee 的 WSN 产生巨大的影响。更重要的是，由于 WSN 节点要求电池驱动和低成

⊖ packet/min：包/分钟，又作 ppm（packet per minute）。

本，所以节点存储器（即RAM）的大小通常约为100KB（例如，本例中使用的JN5139的存储器的大小为96KB），并且在上传需要的嵌入式软件之后输入缓冲区的大小通常小于50KB。WSN节点的有限输入缓冲区不能充分处理这么大的数据率，从而导致大量的数据包丢失。

9.8.3 家庭网关上拒绝服务深攻击的分析

前面讨论的攻击工具用于生成TCP攻击包（每个连接115B），攻击目标为家庭网关。攻击工具攻击未受保护的家庭网关，速率的变化范围为每分钟0～1 200次。结果表明，在没有攻击流量期间，成功创建TCP连接的平均时延为530ms，如图9.15所示。在攻击率为429时，平均时延发生显著变化，为1 802ms。如图9.15所示，攻击率越高，平均连接时延就越高。在每分钟攻击1 090次时，尽管攻击率相对较小时，但平均时延为7 431ms。这个水平的攻击，尽管相对较低，也将导致基于RHS-2通信方法的系统服务大幅降低。

从分析未受保护的家庭网关在受攻击期间的连接时延可以得到，选择3s作为DDS触发抑制机制之前连接时延需要达到的阈值。VH和DDS都集成到前面的实验设置中。针对HAS，实施了每分钟799次的攻击，结果如图9.16所示。

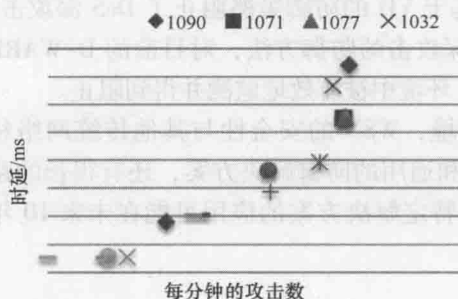


图9.15 未受保护的家庭网关在不同攻击率下的连接时延

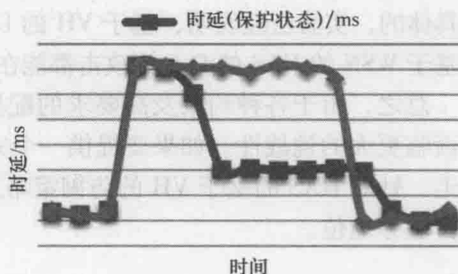


图9.16 VH在每分钟799次DoS攻击操作下的连接时延

如图9.16所示，攻击开始（13:33）时，平均时延迅速从680ms上升至3 500ms。在这点上，VH检测到编码错误和信息重置，说明存在一个潜在的攻击，请求DDS执行一个如第9.6.2节所描述的检测。DDS执行该检测，请求VH由RHS-2方式转换至RHS-1方式。所有这些都发生在3min的时间段内（13:33—13：35）。一旦RHS-2方式转换至RHS-1方式（13:36），受保护的HAS连接时延降至1 515ms。RHS-1方式的路由比通过RHS-2方式的路由平均连接时延更高。因此，对于受保护的VH，攻击开始前，使用RHS-1方式反击攻击比使用RHS-2方式反击攻击的时延更长。在RHS-1方式中，5min（13:36—13:40）后攻击停止。对于这个实验，5min选作用户定义的时间段，即VH状态转化时间（由RHS-1方式至RHS-2方式），检查DoS是

否已经结束。如图9.16所示，5min后，VH将连接由RHS-1方式转换至RHS-2方式，请求DDS执行检测看DoS攻击是否已经结束。在这个实验中，攻击已经结束，所以VH继续使用RHS-2通信方式运行。攻击后，平均时延返回到498~722ms，与攻击开始之前的测量值相似。

9.9 小结

在WSN上有各种各样的安全性攻击，可以划分为主动攻击和被动攻击、内部攻击和外部攻击、传感器级攻击和计算机攻击，以及在不同网络层上的攻击。本章给出了可能的安全攻击和对应的安全转移机制，以及包括ZigBee安全服务在内的安全服务。由于WSN资源受限的特点，在保护WSN免受DoS攻击方面一直面临严峻的挑战。DoS攻击正戏剧性地快速增长，个体攻击也变得更强、更复杂。研究表明，现存的DoS防御方法不能为WSN提供充分的保护。DoS攻击是源于相对资源丰富的共存网络的。维护现有防御的少量的攻击流量可能引起WSN严重的中断、耗尽通信带宽、阻止远程访问WSN。

针对基于WSN的HAS应用，本章对防御策略进行了介绍、实现和评价。该策略集成了VH、RHS和DDS。实验结果表明，基于VH的防御策略阻止了DoS深攻击。更具体的，实验已经表明，基于VH的DoS深攻击的防御方法，对目前的D-WARD和基于WSN的HAS的DoS深攻击都能在VH环境中被有效地监测并得到阻止。

总之，由于各种约束及高要求的配置环境，WSN的安全性与其他传统网络相比面临更大的挑战性。如果要提供一个完善和通用的防御解决方案，还有很长的路要走。针对HAS的基于VH的防御策略这种特定解决方案的应用可能在未来10年内占主导地位。

参考文献

Chan, H., Perrig, A.: Security and privacy in sensor networks. Computer **36**(10), 103–105 (2003)

Chiba, T., Katoh, T., Bista, B.B., Takata, T.: DoS packet filter using DNS information. Proceedings of 20th International Conference on Advanced Information Networking and Applications, Vienna, Austria, April 2006, pp. 6–11

Du, X., Chen, H.: Security in wireless sensor networks. IEEE Wirel. Commun. **15**(4), 60–66 (2008)

Elahi, A., Gschwender, A.: ZigBee Wireless Sensor and Control Network. Prentice Hall, NJ (2009)

Gill, K., Yang, S.H.: Secure Remote Access for Home Automation Systems', Measurement + Control, vol. 41(10), pp. 305–309 (2008)

Gill, K., Yang, S.H., Yao, F., Lu, X.: A Zigbee-based home automation system. IEEE Trans. Consum. Electron. **55**(2), 422–430 (2009)

ITU-T.: Security architecture for open systems interconnection for CCITT applications—recommendation X.800. Available at http://www.itu.int/rec/T-REC-X.800-199103-I/en (1991)

Kwon, T., Hong, J.: Secure and efficient broadcast authentication in wireless sensor networks. IEEE Trans. Comput. **59**(8), 1120–1133 (2010)

Mirkovic, J. Prier, G., Reiher, P.: Source-end DDoS defense. Proceedings of the Second IEEE International Symposium on Network Computing and Applications, Cambridge, MA, USA, April 2003, pp. 171–178

Mirkovic, J.: D-WARD: Source-end defense against distributed denial-of-service attacks. PhD Thesis in University of California (2003)

Ning, P., Liu, A., Du, W.L.: Mitigation DoS attacks against broadcast authentication in wireless sensor networks. ACM Trans. Sens. Netw. **4**(1), 1–35 (2008)

Perrig, A., Stankovic, J., Wagner, D.: Security in wireless sensor networks. Commun. ACM **47**(6), 53–57 (2004)

Ratul, M., Steven, M.B., Sally, F., John, I., Vern, P., Shenker, S.: Controlling high bandwidth aggregates in the network. ACM SIGCOMM Comput. Commun. Rev. **32**(3), 62–73 (2002)

Ricciato, F., Coluccia, A., D'Alconzo, A.: A review of DoS attack models for 3G cellular networks from a system-design perspective. Comput. Commun. **33**(5), 551–558 (2010)

Schuba, C.L., Krsul, I.V., Kuhn, M.G., Spafford, E.H., Sundaram, A., Zamboni, D.: Analysis of a denial of service attack on TCP. Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, USA, May 1997, pp. 208–303

Thomer, M.G., Massimiliano, P.: MULTOPS: A data-structure for bandwidth attack detection. Proceedings of 10th Usenix Security Symposium, Washington, D.C., USA, August 2001, pp. 23–29

Wood, A.D., Stankovic, J.A.: Denial of service in sensor networks. IEEE Comput. **35**(10), 54–62 (2002)

ZigBee Alliance.: ZigBee specification. Available at http://www.zigbee.org. Last Accessed June 2012

第10章 移动目标的定位与跟踪

关键字：移动目标　传感器节点定位　定位跟踪　三角测量　指纹　质心定位

10.1 引言

节点定位功能是 WSN 的重要组成部分，这是由 WSN 固有的特性决定的。WSN 中的定位这一术语被用来辨识产生传感器读数的物理位置。位置信息在大多数 WSN 应用中至关重要，没有获取准确位置信息的测量数据是毫无意义的（Liu 等，2012）。

WSN 的定位与跟踪算法利用一些被称为信标节点或参考节点的已知特殊节点的位置信息估算传感器节点在网络中的位置，即通过被放置在已知位置的节点或使用全球定位系统（Global Positioning System，GPS）获取传感器的绝对位置。传感器节点与信标节点之间的距离可通过测量接收信号强度指示（Received Signal Strength Indicator，RSSI）和链路质量指示（Link Quality Indicator，LQI）来获得。它们两个都是无线电硬件链路的度量量，并且能够通过最小的计算量来确定距离。其他测量距离的方法还有测量到达时间（Time of Arrival，ToA）或是到达时间差（Time Difference of Arrival，TDoA），时间测量的难点在于相关设备的时间同步问题及大量的数学计算（Blumenthal 等，2007），10.2 节将详细阐述测量距离的方法。目前已经提出了许多定位算法来确定传感器的位置信息，10.3 节将介绍三角测量法、指纹定位法、质心定位法和跳计数技术。其他更多的方法可以在相关的文献中找到。10.4 节将介绍两种提高定位准确度的方法：一种方法是提高距离测量质量，另一种方法是根据现有的数据集找到最好的解。10.5 节阐述了基于 ZigBee 的多目标跟踪方法，多目标跟踪问题可以转换成多个单目标跟踪问题去研究。10.6 节提供了地下隧道跟踪研究实例。

最后，在 WSN 定位和跟踪算法设计方面，应该考虑以下几方面的问题：

● 跟踪准确度。不同的应用对于不同的定位跟踪准确度也有不同的要求，重要的是开发满足准确度要求的跟踪系统。

● 能量限制。大多数传感器是电池供电并且能量资源有限。定位和跟踪所涉及的所有处理、通信和感知行为必须是高效节能的，否则将减少传感器设备的使用寿命。

● 信号干扰。同一网络中的节点间干扰，源于同一时刻不同节点的数据包传送冲突。这会降低定位和跟踪所需的信息传输。

● 环境中的障碍物和地形的不规则。这些将导致位置估算不准确。例如，大

的岩石之类的物体可能妨碍视线，阻止 TDoA 和 GPS 测距，或是引起无线电信号的干扰。

● 节点密度。它对于识别算法隐含的密度假设非常重要，因为高节点密度可能是很昂贵甚至完全不可行的。

10.2　距离测定

定位算法要求根据距离去估算未知设备的位置。本节介绍四种获取距离的方法：RSSI，LQI，ToA，TDoA。

10.2.1　接收端信号强度指示

获取距离的一种可能性是测量无线电信号的接收信号强度（Received Signal Strength，RSS）。RSS 基本是指发送装置的发送功率（P_{TX}）直接影响到接收装置的接收功率（P_{RX}）。根据 Friis 的自由空间传输方程（Rappaport，1996），检测到的 RSS“衰减”为发送器-接收器间隔距离的函数。

$$P_{RX} = P_{TX} G_{TX} G_{RX} \left(\frac{\lambda}{4\pi d} \right)^2 \tag{10.1}$$

式中，P_{TX}为发送端传送信号功率；P_{RX}为接收端接收信号功率；G_{TX}为发送器天线增益；G_{RX}为接收器天线增益；λ 为波长；d 为发送和接收装置之间的距离。

在嵌入式设备中，RSS 被转换为 RSSI，它可以表示成所接收信号功率与参考功率的比值（P_{Ref}）。通常，参考功率用 $P_{Ref} = 1\text{mW}$ 绝对值表示。

$$\text{RSSI} = 10\log\frac{P_{RX}}{P_{Ref}}, \text{RSSI 的单位为 dBm} \tag{10.2}$$

接收功率增加导致 RSSI 的增加。因而，距离 d 间接和 RSSI 成反比。理想的 P_{RX}分布在实际中并不适用，因为无线电信号的传播可能受到其他干扰因素的影响：

● 金属物体的反射；

● 其他电磁场；

● 不同传播速度媒介的折射；

● 障碍物；

● 不适用的接收电路。

这些影响明显降低了 RSSI 的质量。因此，在许多应用中，RSSI 有较高方差并且质量明显降低。

根据式（10.1）和式（10.2），无线电设备发出的信号强度和信号传送的距离存在指数关系。实际上，这种相关性被证实是不完美的，但是它仍然存在，原因在于有效的无线信号传播特性不同于该算法假定的理想的理论关系。上面提到的影响，如反射、衰减和多径效应，可能大大地影响信号传播的效果。

10.2.2 链路质量指示

确定距离的另一个方法是基于信号传输的 LQI。根据 IEEE 802.15.4，LQI 是接收的数据包的强度和质量的特性描述。LQI 测量每一个成功接收到的数据包并且产生 0 ~ 255 范围的整数（0×00 ~ 0×ff），指示由接收装置检测到的最低和最高质量的信号。

需要注意的是，LQI 只适用于支持 IEEE 802.15.4 的设备，扩展链路质量的 LQI 必须由软件来完成。信号强度和链路质量值没有必然的联系，但是如果 LQI 低的话，有可能 RSSI 也会偏低。因此，大多数时候需要重视 RSSI。

10.2.3 信号到达时间

ToA 是基于两个节点之间信号传播的时间去估算距离的。通常，超声波信号被引入到基于 ToA 的定位系统中，如图 10.1 所示。在通信系统中，ToA 系统要求拥有一个高精度的时钟。发送装置和接收装置之间的距离可以使用下式来计算：

$$d=\frac{[(T_3-T_0)-(T_2-T_1)]v}{2} \tag{10.3}$$

式中，T_0、T_1、T_2、T_3和 v 分别为超声波信号的瞬时时间和速度。

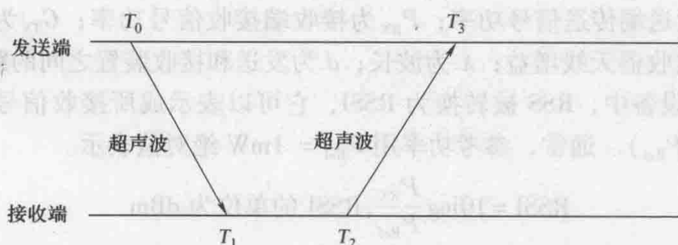


图 10.1 ToA 方法

10.2.4 信号到达的时间差

TDoA 是基于两个以不同速度传播的无线电信号，如 RF 和超声波，来估算距离的。两个节点之间的距离可以通过测量发送时间和接收时间的差异来估算，如图 10.2 所示。

发送装置和接收装置之间的距离 d 可以使用下式来计算：

$$d=(T_{US}-T_{RF})\left(\frac{v_{RF}\,v_{US}}{v_{RF}-v_{US}}\right) \tag{10.4}$$

式中，v_{RF}、v_{US}分别为 RF 的传播速度和超声波信号速度；T_{US}和 T_{RF}分别为通过超声波和 RF 传播的时间。

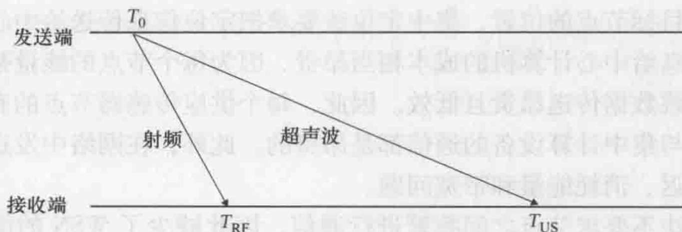


图10.2　TDoA方法

10.3　定位方法

许多提供节点定位信息的定位算法已经被提出来，关于被用来估算位置的工作机制，定位策略可以分成两种：基于距离的定位方法和不基于距离的定位方法。前者是通过协议定义的，使用点对点距离估算或是角度估算去计算位置；后者则没有对这些信息的可用性和有效性进行假设。由于WSN设备硬件的限制，人们正在寻求一种不基于距离的定位方法代替更昂贵的基于距离的方法。关于在哪执行定位计算的问题，相关这些定位协议可以划分成集中和分散两种方法。集中定位要求传送测量信息给中心节点，然后由中心节点去计算目标位置；分散式定位分配位置计算给相应的节点，并且只需要传送最新的目标坐标给中心节点，如图10.3所示。

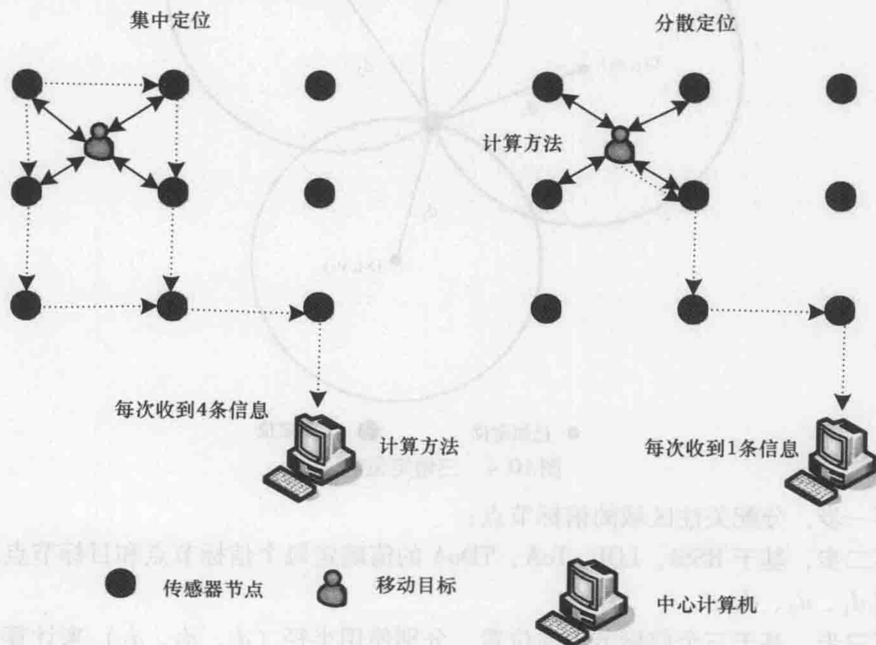


图10.3　集中与分散定位方法

为了计算目标节点的位置，集中定位法要求把定位信息传送给中心节点。传送目标的定位信息给中心计算机的成本相当昂贵，因为每个节点的能量是有限的，而且长距离的多跳数据传送昂贵且低效。因此，每个供应传感器节点的有限的能量供应意味着任何与集中计算设备的通信都是昂贵的。此外，在网络中发送时间序列数据还会产生延迟、消耗能量和带宽问题。

分散定位法不要求节点之间频繁进行通信，因此减少了 WSN 的能量消耗。然而，分散定位系统要求每一个移动目标都有硬件设备，以便从信标节点搜集定位信息、计算它们的位置、传送它们的当前位置给中心计算机。

10.3.1 三角定位法

三角定位法是通过测量从三个不同的已知点到目标点的距离来定位目标点的方法。如果三个信标节点（已知坐标位置的节点）和目标节点（未知坐标位置的节点）之间的距离 d 可以测量，那么可以画出以 d 为半径的圆，如图 10.4 所示。这三个圆有且只有一个交点，这个点就是目标节点的位置。三角测量法包括以下步骤：

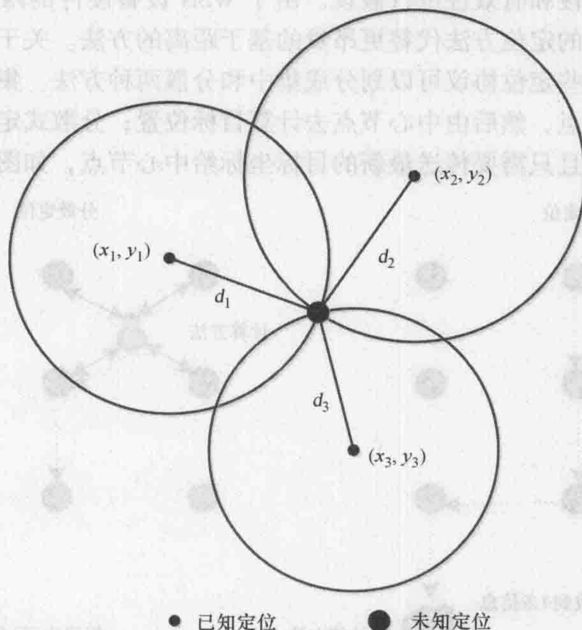


图 10.4 三角定位法

第一步，分配关注区域的信标节点；

第二步，基于 RSSI、LQI、ToA、TDoA 的值确定每个信标节点和目标节点之间的距离 d_1、d_2、d_3。

第三步，基于三个信标节点的位置，分别使用半径（d_1，d_2，d_3）来计算目标节点的位置。

如果（d_1，d_2，d_3）是准确已知的，则存在以下三式：

$$(x_1-x)^2+(y_1-y)^2=d_1^2 \tag{10.5}$$

$$(x_2-x)^2+(y_2-y)^2=d_2^2 \tag{10.6}$$

$$(x_3-x)^2+(y_3-y)^2=d_3^2 \tag{10.7}$$

结合上面任意两式，将得到两组（x，y）。使用第三式，另外唯一的一组（x，y）也可以被确定。不幸的是，实际情况不是这么简单，三个半径（d_1，d_2，d_3）总是不够准确，所以需要付出更多的努力去确定目标节点的位置（x，y）。

10.3.2　指纹定位法

指纹定位法是一种基于信号传播行为和被分成许多小网格的跟踪现场的几何信息的一种方法。定位指纹是通过确定信号在每个网格点的行为表现而工作的，即每个网格的多径结构。

指纹定位法的实施通常分为两个阶段，如图10.5所示。第一个阶段，即离线阶段，包括在不同的坐标系下测量移动物体的位置，并且在数据库中存储收集到的信息。离线算法包括以下步骤：

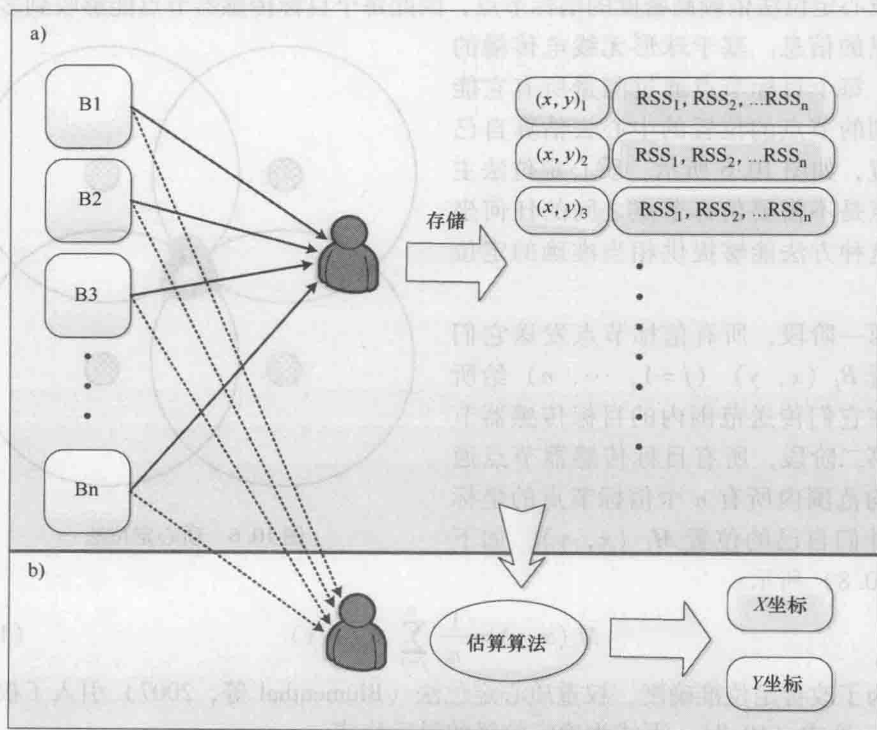


图10.5　指纹方法（离线和在线阶段）

a）离线阶段　b）在线阶段

第一步，在跟踪区域分配信标节点 B_1，B_2，…，B_n；

第二步，把跟踪区域划分成许多小的网格，并且在跟踪区域使用网格点作为参考点 $(x, y)_1$，$(x, y)_2$，$(x, y)_3$，…；

第三步，从信标点得到每个参考点的 RSS 值，并且用相应的定位坐标把它们存储到数据库中。

另一个阶段，即在线阶段，移动目标从它所处区域内的不同信标节点收集若干 RSS 值并且把它们发送给一个服务器。服务器应用一个在线搜索算法去估算移动目标的位置（Alhmiedat 和 Yang，2011）。在线算法包括以下步骤：

第一步，移动目标进入跟踪区域，然后从每个信标节点收集 RSS 值；

第二步，把采集到的 RSS 值和数据库中存储值相比较；

第三步，在数据库中检索最接近的 RSS 值的位置。

由于离线阶段的成本原因，对于一个大的跟踪区域每个网格的大小不能足够小，所以确定移动目标正确位置的某些误差仍然一直存在。

10.3.3 质心定位法

质心定位法依赖高密度的信标节点，因此每个目标传感器节点能够收到多个信标节点的信息。基于球形无线电传播的假设，每个目标节点通过测量所有它能接收到的节点的位置的中心去估算自己的位置，如图 10.6 所示。质心定位法主要优点是不需要信标节点之间的任何坐标。这种方法能够提供相当准确的定位信息。

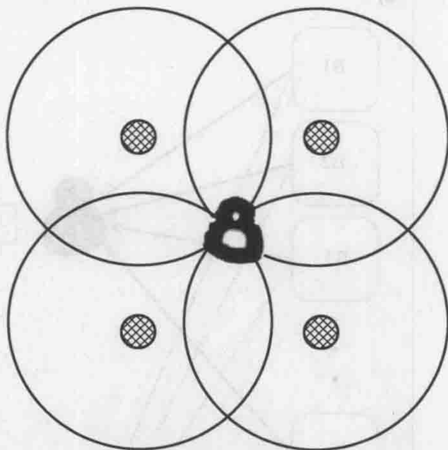


图 10.6 质心定位法

第一阶段，所有信标节点发送它们的位置 B_j（x，y）（$j=1$，…，n）给所有的在它们传送范围内的目标传感器节点。第二阶段，所有目标传感器节点通过平均范围内所有 n 个信标节点的坐标位置计们自己的位置 M_i（x，y），如下式（10.8）所示：

$$M_i(x,y) = \frac{1}{n} \sum_{j=1}^{n} B_j(x,y) \tag{10.8}$$

为了改善定位准确度，权重质心定位法（Blumenthal 等，2007）引入了权重函数 w_{ij}，见式（10.8）。下式为确定位置的最后公式：

$$M_i(x,y) = \frac{1}{\sum_{j=1}^{n} w_{ij}} \sum_{j=1}^{n} [w_{ij} B_j(x,y)] \tag{10.9}$$

权重函数 w_{ij} 依赖距离和目标节点接收器的特性。由于环境情况的变化，每一个应用情形要求有不同的权重函数，短距离的权重大于长距离的权重是合理的。因而，目标节点 M_i（x，y）和信标节点 B_j（x，y）之间的权重 w_{ij} 和距离 d_{ij} 是呈反比的。作一个近似，可以得到下式：

$$w_{ij} = \frac{1}{d_{ij}} \tag{10.10}$$

为了体现权重越高距离越低，距离被提升到指数 g（$g \geqslant 1$）的高度。所以式（10.10）变成下式：

$$w_{ij} = \frac{1}{d_{ij}^g} \tag{10.11}$$

根据应用情形，最优 g 可以被明确地确定。

10.4　定位准确度的提高

应用上述定位方法所面临的挑战，主要集中表现在处理由于应用环境的改变和无线电信号传播属性所带来的距离测定的不确定性上。本节将分别介绍环境因素以说明应用环境中的动态变化消除 RSSI 异常值的预处理 RSSI 方法，以及为了提高准确度而最优考虑所有距离的进化优化方法。

10.4.1　环境因素的引入

目标所处的跟踪环境大部分情况下是动态的，如在室内环境中人的走动和家居的重新摆设、室外环境中每日天气的变化等。用每对信标节点间的已知距离和实时的 RSS 测量值如式（10.12）所定义来描述环境，式中的 ef_{ij}（Alhmiedat 和 Yang，2008）称为环境因素。

$$\mathrm{ef}_{ij} = \frac{\mathrm{RSS}(B_i, B_j)}{d(B_i, B_j)} \tag{10.12}$$

式中，$\mathrm{RSS}(B_i, B_j)$ 为信标节点 B_i 和 B_j 之间的 RSS 值（RSSI 或 LQI），而 $d(B_i, B_j)$ 表示它们之间的距离，该距离是已知的。获得唯一的环境因素最简单的方法是将 μ_{ef} 作为各个环境因素的平均值：

$$\mu_{\mathrm{ef}} \frac{\sum_{j=1, i \neq j}^{n} \mathrm{ef}_{ij}}{n} \tag{10.13}$$

式中，n 为覆盖目标跟踪区域的信标节点的个数。图 10.7 给出了环境因素示例，有一个拥有三个信标节点（B_1，B_2，B_3）的环境的环境因素和一个已经定位的移动目标 M。唯一的环境因素可以由多种方法得出，最直接的方法是通过图 10.7 给出的 μ_{ef} 分割它们将 RSSI 或 LQI 的值转换成距离。

$$d_{B_iM} = \frac{\mathrm{RSS}(B_i, M)}{\mu_{\mathrm{ef}}}, i = 1, 2, 3 \tag{10.14}$$

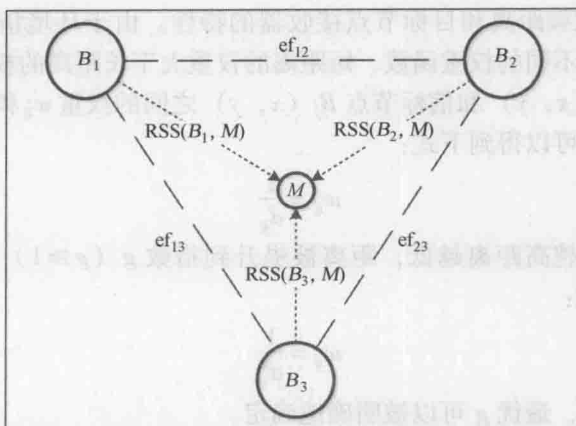


图 10.7 环境因素示例

10.4.2 无线信号异常值的消除

用于确定 RSSI 或 LQI 的无线信号不可避免地受许多环境因素的影响，如反射、障碍物和其他电磁场。因此，任何测量 RSSI 和 LQI 的方法都包含一些随机的因素，消除这些噪声因素将有助于提高定位的准确度。

下面将使用 RSSI 的值作为例子，但相同的处理可以应用于其他的测量定位，如 LOI 的定位。Dixon 方法（Feng 等，2012）在这里被用来消除 RSSI 的异常值。每个时刻接收到的所有的 RSSI 值的标准差被记作 R_{SD}，标准差的阈值定义为 T_{SD}。从 RSSI 测量得到的 RSSI 值记作 R_{avg}，有

$$R_{avg} = \alpha R_{avg1} + (1-\alpha) R_{avg2} \tag{10.15}$$

其中

$$R_{avg1} = \frac{1}{m}\sum_{i=1}^{m} R_i, \quad R_i \leqslant \frac{1}{q}\sum_{j=1}^{q} R_j \tag{10.16}$$

$$R_{avg2} = \frac{1}{q-m}\sum_{i=1}^{q-m} R_i, \quad R_i > \frac{1}{q}\sum_{j=1}^{q} R_j \tag{10.17}$$

式中，m 为 RSSI 的值的数目，它小于等于 q 的 RSSI 值；α 为根据以下式计算得来：

$$\alpha = \begin{cases} 0.5\left(\dfrac{T_{SD}-R_{SD}}{T_{SD}}+1\right), R_{SD} \leqslant T_{SD} \\ 0.5\left(1-\dfrac{R_{SD}-T_{SD}}{T_{SD}}\right), R_{SD} > T_{SD} \end{cases} \tag{10.18}$$

T_{SD}的大小取决于具体的环境。目标节点根据一系列接收的 RSSI 值得到 R_{SD}，每次都将 R_{SD}的值与 T_{SD}的值进行比较。如果 $R_{SD} \leqslant T_{SD}$，则获取的 RSI 值是稳定的。从式

(10.18) 可以计算出 α 的值，$\alpha \in (0.5, 1)$。如果 $R_{SD} > T_{SD}$，则获取的 RSSI 值是不稳定的，按照式 (10.18) 可以计算出 α 的值，$\alpha \in (0, 0.5)$。按照式 (10.15) ~式 (10.17)，可以消除了异常的 RSSI 值。

10.4.3 进化优化算法

在图 10.4 所示的三角测量法中，目标节点的位置可以从它与邻近的信标节点之间的距离信息计算得到，这些信标节点的坐标信息为

$$(x - x_i)^2 + (y - y_i)^2 = d_i^2, i = 1, 2, \cdots, N \tag{10.19}$$

式中，(x, y) 为目标节点的坐标；(x_i, y_i) 为第 i 个信标节点的坐标；d_i 为目标节点与第 i 个信标节点之间的距离；N 为信标节点的个数。

在无噪声系统中，每次距离的测定都是指定一个目标节点可能位置的圆，这些圆的交点确定且唯一确定一个目标位置。这种几何技术称为三角测量，在系统存在噪声的情况下，由于错误的距离测定，式 (10.19) 定义的圆可能会相交出多个点，则采用模糊解决方案，如图 10.8 所示。

因此，定位问题就变成一个搜索问题，通过最小化计算距离和测量距离之间的差，来搜索目标节点坐标的估算值 $(\hat{x}, \hat{y})$。一种流行的统计定位算法是非线性最小二乘法 (Nonlinear Least Square，NLS) 技术，通过此技术目标节点位置的计算如下：

$$(\hat{x}, \hat{y}) = \arg\min_{(x,y)} f(x, y) = \arg\min_{(x,y)} \sum_{i=1}^{N} \beta_i \left(\sqrt{(x - x_i)^2 + (y + y_i)^2} - d_i \right)^2 \tag{10.20}$$

式中，$f(x, y)$ 为成本函数；N 为信标节点的个数；β_i 为第 i 个测量值的加权系数，它通常反映了测量值的可靠性。式 (10.20) 的求解通常需要用如最速下降法和高斯-牛顿法 (Cheng 等，2005) 这种数值搜索方法。这两种方法都具有较高的计算复杂度，并且通常需要一个良好的初始值以避免收敛到局部极小的成本函数。另外，线性最小二乘估算法 (Linear Least Square Estimation，LLSE) 能够提供具有较低计算复杂度的相对优化的位置估算，但是其准确度较差。

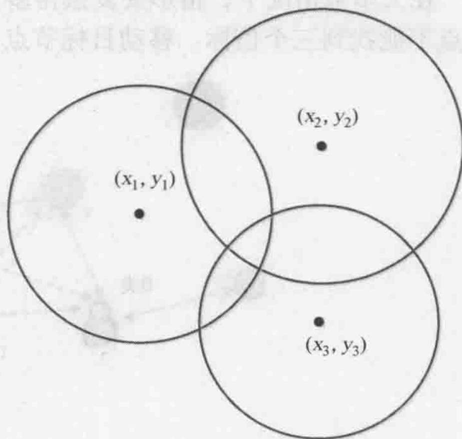


图 10.8 由于距离测量错误所产生的三角区域多重交叉

10.5 多移动目标跟踪

多移动目标跟踪通常是许多应用所需要的。在多移动目标跟踪中，关键的挑战是在相邻的区域是否能够拥有足够的信标节点；以及如果没有足够的信标，如何使用一些位置已经确定的移动目标节点作为额外信标。

如图 10.9 所示，两个移动目标（m_1 和 m_2），在一个 ZigBee 传感器现场，通过一个路由器和两个终端设备相连接形成的三角形。在这种情况下，跟踪多个移动目标节点可以通过把多目标场景划分成一系列单移动目标跟踪来实现。

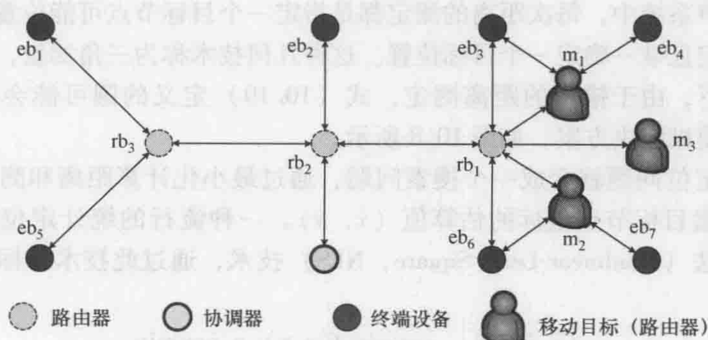


图 10.9 两个移动目标在一个 ZigBee 传感器现场

在大多数情况下，情形要复杂得多，并且在图 10.10 所示的通信范围内移动节点不能找到三个信标。移动目标节点 1（A 类）在它的范围内包含三个信标；

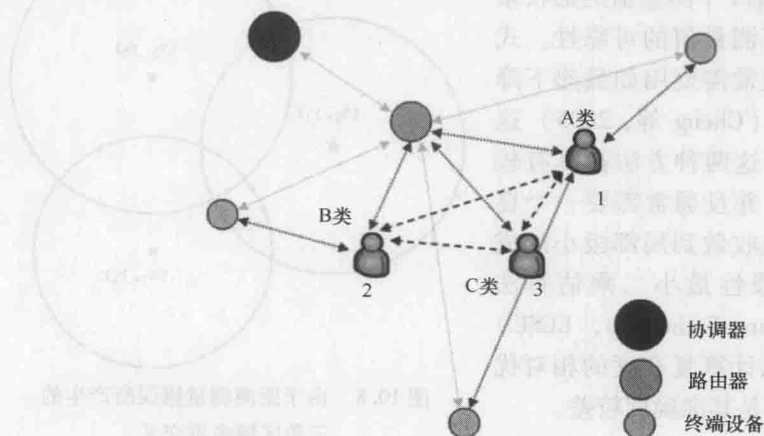


图 10.10 在一个 ZigBee 网络中的多个移动目标节点跟踪

然而，移动节点 2（B 类）只有两个信标；移动节点 3（C 类）只有一个信标。在这种情况下，一个先前已经确定位置的移动节点可以被用作额外的参考节点。“先到先服务”原则被用于分配移动目标节点作为参考节点。等级 A 提供最好的定位准确度，因为移动目标节点被三个已知位置的信标点覆盖。B 类的跟踪准确度比 A 类低，因为移动目标节点只被两个已知位置的信标点和一个先前已经确定位置的移动目标节点覆盖。C 类提供了更差的跟踪准确度，因为移动节点只被单独的一个信标节点和其余的可利用的参考节点所覆盖。这些参考节点是先前已经确定位置的移动目标节点，误差将是 B 类和 C 类的累积。

10.6　案例研究：地下隧道移动目标跟踪

由于下面的特性，对于 WSN 定位的应用，地下隧道是相当有挑战性的环境。（1）地下隧道的空间形状非常狭长，这意味着 WSN 的部署是线形或是链形并且是低密度的；而且由于多跳，数据传输是个非常耗能的过程。（2）由于水和灰尘，空气是潮湿、肮脏的，这很明显影响了无线通信距离的有效性。（3）地下隧道表面通常是粗糙的，无线电波的多径效应严重。图 10.11 给出了一个地下煤矿隧道环境。



图 10.11　一个地下煤矿隧道环境

由于特殊的地理限制，部署在地下隧道的基于 WSN 的定位系统具有链形拓扑结构。图 10.12 所示为定位系统的结构，包括一个上位 PC 作为监测站、一个协调器、参考节点（在这被称作锚节点）和一个或是多个移动目标节点（这里所谓的盲节点）。

协调器负责建立网络。它也作为通过一系列端口到达上位 PC 的一个网关。上位 PC 负责锚节点配置和定位数据的管理。锚节点是 ZigBee 网络的路由器，它们从隧道环境中采集数据和参与定位。当在一跳范围内接收到一个盲节点的定位要求时，锚节点用它们的 ID 标识和坐标进行响应，并且使 RF-TOF 引擎为范围测定做

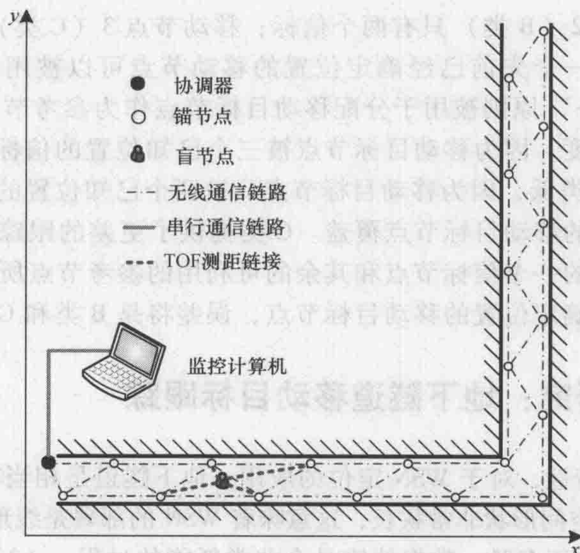


图 10.12 定位系统的结构（Qin 等，2012）

好准备。盲节点也是 ZigBee 的路由器，它需要在通信范围内与多个锚节点直接通信，盲节点执行定位算法。

为了确保网络通信有一定的冗余，并且在一跳范围内盲节点能找到足够的锚节点，锚节点应该沿隧道两侧部署。在同一侧任意两个邻居节点之间的距离应该保持相同，并且应该小于任意两个节点之间的有效通信距离。对面的锚节点应该被交替放置。换句话说，一侧的一个锚节点应该放置在对面两个锚节点之间，如图 10.12 所示。

在这个应用中，三个优化的方法都已经被实现，LLSE（Gezici 等，2008）、七个潜在估算（Seven Potential Estimation，SPE）（Merhi 等，2009）、粒子群最优估算（Particle Swarm Optimization Estimation，PSOE）（Eberhart 和 Shi，2001）。这里省略掉细节。图 10.13 给出了三个定位算法的平均定位误差的比较，三种算法曲线都有相似的趋势，这意味着大的范围误差很可能降低这些算法的性能，

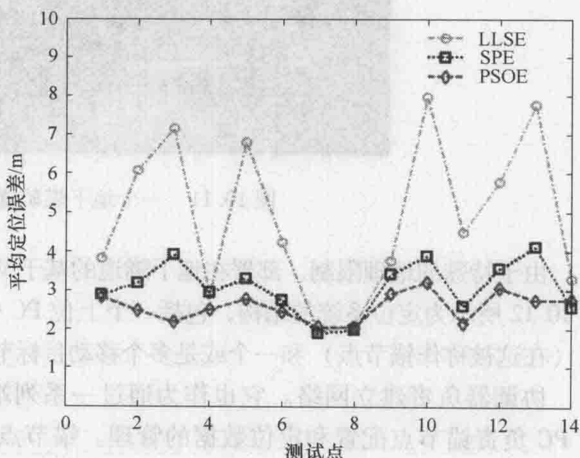


图 10.13 三个定位算法的平均定位误差的比较

但是 PSOE 测距误差的鲁棒性比其他两种算法更强。

10.7　小结

尽管还有更多定位方法在本章没有被讨论，但是基于 WSN 定位的核心技术和大部分基本理论已经介绍。总之，距离测定可以通过无线电信号（如 RSSI 或 LQI），或是定向的传播时间（如 ToA 或 TDoA）来实现。根据它们的通信载荷和计算的位置可以把定位方法分为集中法和分散法。根据是否使用绝对的点对点距离估算位置，它们也可以分成基于距离或是与距离无关的方法。三角测量是基于距离的方法，但是指纹和质心定位属于与距离无关的种类。定位最大的挑战是定位准确度通常很差，本章提出了三种改善准确度的方法，也就是考虑到环境变化的不确定性，消除 RSS 的异常值，以及找到定位的最优方法。如果在通信范围内存在三个或是更多的参考节点，多数移动目标跟踪可以划分成一系列单目标跟踪；否则，先前已经被定位的移动目标不得不被用作附加的参考节点，即使估算误差已经累积到了定位计算中。

参考文献

Alhmiedat, T., Yang, S.H.: A ZigBee Based Mobile Tracking System through Wireless Sensor Networks. Int. J. Adv. Mechatron. Syst. **1**(1), 63–70 (2008)

Alhmiedat, T., Yang, S.H.: Tracking mobile targets through wireless sensor networks, p. 47. Lap Lambert Academic Publishing, Saarbrücken (2011)

Blumenthal, J., Grossmann, R., Golatowski, F., and Timmermann, D.: Weighted centroid localization in Zigbee-Based sensor networks. In: IEEE International Symposium on Intelligent Signal Processing, pp. 1–6 (2007)

Cheng, B., Hudson, R., Lorenzelli, F., Vandenberghe L., Yao, K.: Distributed gauss-newton method for node localization in wireless sensor networks. In: IEEE Sixth Workshop on Signal Processing Advances in Wireless Communication, pp. 915–919 (2005)

Eberhart, R.C., Shi, Y.: Particle swarm optimization: developments, applications and resources. In: Proceedings of the IEEE Congress on Evolutionary Computation, Seoul, Korea, pp. 81–86 (2001)

Feng, W.J., Bi, X.W., Jiang, R.: A novella adaptive cooperative location algorithm for wireless sensor networks. Int. J. Autom. Comput. **9**(5), 539–544 (2012)

Gezici, S. Guvenc, I., Sahinoglu, Z.: On the performance of linear least-squares estimation in wireless positioning systems. In: IEEE International Conference on Communications, pp. 4203–4208 (2008)

Liu, Y., Yi X., He, Y.: A novel centroid localization for wireless sensor networks. Int. J. Distrib. Sens. Netw. Available online at http://1/dx.doi.org/10.1155/2012/829253 (2012)

Merhi, Z., Elgamel, M., Bayoumi, M.: A lightweight collaborative fault tolerant target localization system for wireless sensor networks. IEEE Trans. Mob. Comput. **8**, 1690–1703 (2009)

Qin Y., Wang F., Zhou, C., Yang, S.H.: A particle swarm optimization based distributed localization scheme in tunnel environment. Wireless Sensor Systems—IET Conference, June, London (2012)

Rappaport, T.S.: Wireless communications: principles and practice. Prentice-Hall Inc, New Jersey (1996)

第 11 章　面向物流管理的无线射频识别/无线传感器网络的混合网络

关键词：射频识别　混合传感器网络　网络架构　物流管理

11.1　引言

在任何物流管理系统的设计中，都需要回答 4W 问题（Who、What、When 和 Where）。本章的重点是通过建立一个混合的 RFID[⊖]/WSN 网络提供对这些 4W 问题的回答。

因具有感知能力，一个 RFID 系统能够响应和感知资产状况和环境条件，从而不仅能够确定供应链中的特定商品所处的特定位置，而且能够确定这些商品是否处在适当的条件下（Pradhan，2005）。不同类型的 RFID 系统可以被集成在一个混合的 RFID /WSN 中，以满足更多复杂的物流应用。本章介绍了在复杂的混合物流应用中，设计、开发、实现和评价一个整合的 RFID 传感器网络的最新研究成果。在这个整合网络中，同类型的 RFID 系统和 WSN 被集成到一个统一的框架中。

11.2　无线射频识别技术

无线射频识别（RFID）技术是 Auto-ID 技术之一。Auto-ID 是自动识别技术的简称，它是指机器能够识别物体技术的一个广义术语。代替员工识别物体并手动将信息输入计算机，Auto-ID 技术的关键因素是自动捕获数据的能力。主要的几种 Auto-ID 技术包括，条形码、智能卡、语音识别、视网膜或指纹扫描、光学字符识别（Optical Character Recognition，OCR）以及 RFID。

RFID 是一种利用无线电波来自动地识别人或物体的技术的通称。相对于其他 Auto-ID 技术，RFID 系统有自身的特点：RFID 系统提供了一种在标签和读取器之间的非接触数据传输方式，代替了手动输入或扫描识别码，无需无障碍和视距读取；标签信息可以重写并且标签本身可以回收再利用；多个标签可以同时通过一个 RFID 读取器读数，被称为标签的批量读取，这使得识别工作更加高效；RFID 标签

⊖ RFID：无线射频识别，Radio Frequency Identification。

可以很容易地被分解，比印刷的条形码更可靠。

一个典型的 RFID 系统的基本组成部分：信号发射机或标签，是一个在必要时通过连接的天线储存和传输唯一序列码的芯片；RFID 读取器，用于接收和识别由标签发送的信息；本地服务器，读取器提供信息给它，由一个管理系统处理这些从标签收集到的数据。图 11.1 给出了典型的 RFID 系统。本章主要研究标签和读取器层次的问题。

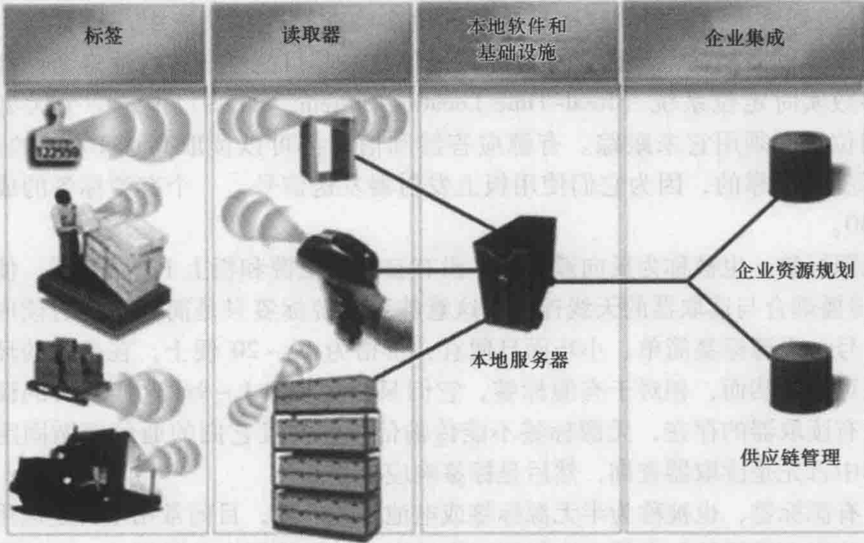


图 11.1　典型的 RFID 系统

11.2.1　无线射频识别标签

一个标签的意义在于物理储存识别数据信息和附加信息，标签还具有进行数据通信的能力，因此它可以被读取。依据电源的使用 RFID 通常有三种类型，分为有源，无源和半无源/半有源标签。表 11.1 给出了不同的 RFID 标签的比较。

表 11.1　不同的 RFID 标签的比较（Yang 和 Yang，2007）

特　点	无 源 标 签	半无源/半有源标签	有 源 标 签
用于数据传输的电源	否	否	是
芯片本身的电源	否	是	是
与读取器通信	反向散射	反向散射	RF 发送
读取范围	短	中	长
标签成本	低	中	高

有源标签具有板上发射器，并使用电池作为电源；它们通过发射器发送 ID 码，拥有一个广泛的读取范围。有源标签一般工作在 455MHz、2.45GHz 或 5.8GHz，通常具有 20 ~ 100m 的读取范围。因为它们有超长距离跟踪物体的能力，所以通常被用于跟踪大型资产目标，如集装箱、车辆和飞机。

两种典型的有源标签是应答器和信标。有源应答器不是自发地发送信息，只有当一个来自读取器设备的信号被接收时，它才从睡眠模式被唤醒，然后把标签的 ID 发送到这个读取器。这些标签通常用在检查站控制系统中，只有当一个标签处于某个读取器的范围内，标签才广播信息，其目的是节省电池寿命。信标用于大多数实时定位系统（Real-Time Locating System，RTLS）中，一个大型资产的精确位置必须用它来跟踪。有源应答器和信标都可以读取高达 100m 的范围，读取标签是可靠的，因为它们使用板上发射器发送信号，一个有源标签的成本为 £ 5 ~ 30。

无源标签，也被称为反向散射器，没有自己的电源和板上 RF 发射器，使用感应式/传播耦合与读取器的天线连接，这意味着无源标签只是简单地反射读取器发出的信号。无源标签简单、小巧而且便宜，价格为 10 ~ 20 便士，在恶劣的环境条件下更可靠。然而，相对于有源标签，它们只能实现 0.1 ~ 9m 这样较短的读取范围。没有读取器的存在，无源标签不能传输信息，并且它们的通信遵循固定的模式，其中首先是读取器查询，然后是标签响应查询。

半有源标签，也被称为半无源标签或电池辅助标签，目前常用于特定应用的场合。这些半有源标签包含的电池仅用于支持嵌入式存储器和传感器。一个读取器和标签之间的通信遵循与无源标签相同的方法，这意味着标签从读取器发送信号获得能量，再反射信号返回到它。像无源标签一样，其通信总是开始于读取器的查询，然后标签作出回应。它们可以在长达 30m 的距离被读取，比无源标签具有更长的响应距离。此外，在金属和液体存在的环境下其性能也比无源标签好得多。半有源标签不需要时间收集能量来激活标签芯片，所以更快的读取速度是半有源标签的另一个优势。

11.2.2 无线射频识别读取设备

无论使用哪个类型的标签，它们只存储与它们所附着物体的数据，在许多实际的应用中需要根据要求将数据读取并发送到一个服务器或网络上。一个读取器，也被称为一个询问器，它是与标签通信的设备，执行如读取和写入标签的低级别事件，然后将这些事件的结果发送到服务器上。读取器可以是固定或手持的设备。典型的 RFID 读取器组件包括天线、RF 收发器、微控制器、通信接口和电源。

11.3　无线射频识别与传感器的混合网络

RFID 系统可以在硬件或软件层面上与 WSN 进行集成。硬件层面的集成是通过把 RFID 应答器与传感器节点嵌入到相同的印制电路板上来整合传感器与 RFID 读取器，因此，传感器与 RFID 读取器设备共同工作实现 RFID 和 WSN 的功能。软件层面的集成允许 RFID 网络和 WSN 实现网络层的协作，这部分只考虑软件层面的集成。

11.3.1　读取式传感器

为把 RFID 系统和 WSN 结合起来，“传感器”的概念需要扩展。通常传感器是响应特定类型环境条件的激励并获得特定物理量测量的装置。在 RFID/传感器网络中，扩展了传感器的概念，将 RFID 读取器设备作为传感器看待。读取器设备所感知的是外观表现，即在读取范围内接近或通过 RFID 应答器/标签。在这种情况下，该 RFID 读取器和传感器网络中的传感器节点（单元）被认为处于系统结构中的同一层。传感器网络网关设备，如传感器协调器，也将作为 RFID 读取器和中央服务器/网络之间的网关设备。所有由读取器产生的信息将经由传感器网关设备被发送到中央服务器。“读取器作为感应器”的体系结构如图 11.2 所示。

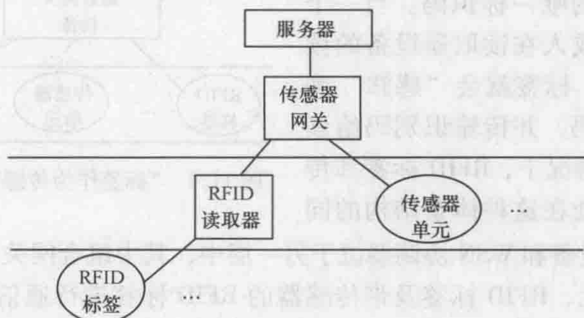


图 11.2　“读取器作为感应器”的体系结构

虽然不同的接口和协议，如 RS-232、RJ-45 或 Wi-Fi 都适用于桥接读取器和传感器网络网关设备，但是 WSN 协议（IEEE 802.15.4 或 Zigbee）才能使读取器真正成为 WSN 节点。“读取器作为传感器”的概念已经被使用在一些出版物上（Englund 和 Wallin，2004；Mason 等，2006）。

图 11.3 所示为“读取器作为传感器”体系结构的应用实例。许多 RFID 读取器被部署在仓库中执行物体识别、访问控制和实时定位跟踪任务；每个 RFID 读取器都被赋予了 RF 收发器和 RF 天线来实现无线通信功能。无线传感器节点也被部署在仓库中来调查环境条件和事故。WSN 协议被应用于由 RFID 读取器和传感器节

点所构成的无线 Ad-hoc 网络。这种体系结构最可能的情况是将 RFID 系统集成到一个 WSN 结构的上层。

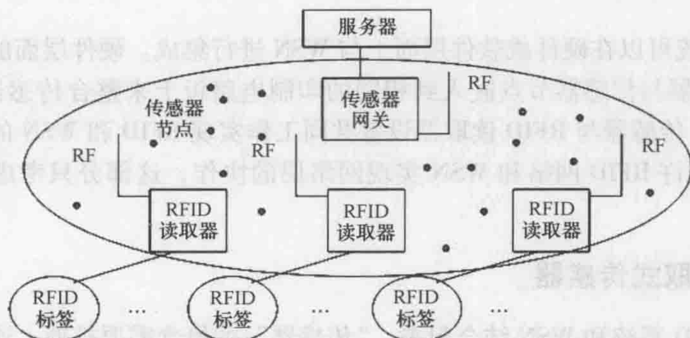


图 11.3 "读取器作为传感器"体系结构的应用实例

11.3.2 标签式传感器

在图 11.4 所示的"标签作为传感器"的体系结构中，"传感器"的概念被扩展到将 RFID 应答器/标签设备作为传感器对待。应答器设备"感知"的是存储在标签存储器中的唯一标识码。当一个带有标签的资产或人在读取器设备的读取范围内移动时，标签就会"感知"到资产或人的识别码，并传输识别码给读取设备。在这种情况下，RFID 标签和传感器单元被认为处在这种体系结构的同一层中。读取器设备和 WSN 协调器位于另一层中，其中组合网关（Gateway，GW）设备与传感器单元、RFID 标签及带传感器的 RFID 标签进行通信。这种类型的组合网关读取器设备的例子已经在 RFID 读取器部分给出。如果在一个网络中只使用 RFID 传感器节点，它们的工作都类似典型的 WSN 节点，所以该组合网关设备只要做一些轻微的修改就能作为 WSN 网关使用。

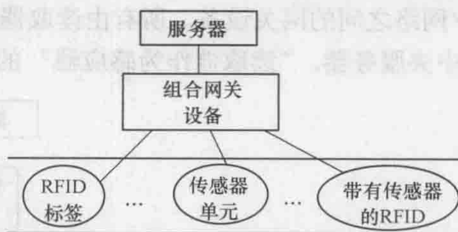


图 11.4 "标签作为传感器"的体系结构

11.4 通用无线射频识别与传感器混合网络体系结构

无源标签是解决廉价及非再生货物大规模实施的最切实可行的办法。因此无源系统最适合应用在"读取器作为传感器"的结构中；另一方面有源 RFID 标签则很容易被纳入"标签作为传感器"的结构。没有任何标识的个体传感器节点则可以工作于两种体系结构中的某一个适当的层。"标签作为传感器"体系结构

中不需要任何额外的读写设备，因此可以符合中小型应用的成本效益要求。对于大型应用，当标签成本变得更加重要时“读取器作为传感器”体系结构则是更好的选择。

一般情况下，上述两种体系结构可以表示为一个统一的混合 RFID/WSN 系统，如图 11.5 所示。这种体系结构有三个层次。从 RFID 方面来讲，服务器层在顶部，读取器层在中间，标签层在底部。从 WSN 方面来说，网络协调器是顶层，网络路由器在中间，各个传感器节点在底部。如本书第 2 章所述，个体传感器节点不需要相互进行通信，但能够和它们的父传感器相互通信。这里，不期望 RFID 标签和传感器节点在标签层中相互通信，但它们可以在读取器层与它们的读取器或路由器相互进行通信。在通信范围内，所有的读取器和网络路由器都被要求能够相互通信，即读取器层形成网状网络。服务器位于顶部，管理 RFID 读取器和网络路由器。

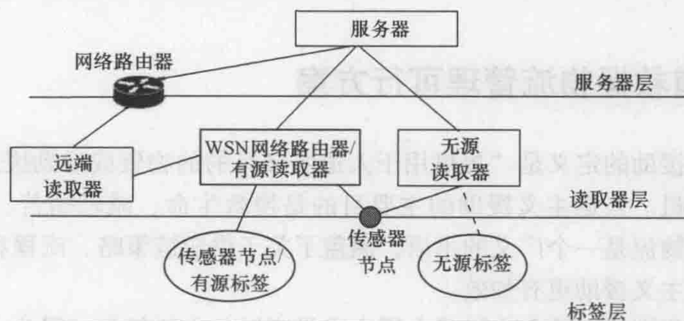


图 11.5　集成混合传感器网络体系结构

除了无源 RFID 标签和它们的读取器之间的通信，在这种集成式体系结构中，网络内部的所有通信要求如 Zigbee 的 WSN 协议的支持。这种混合 RFID 传感器网络的集成体系结构实际上是一个“读取器作为传感器”和“标签作为传感器”体系结构的组合。因此，它可以从两种体系结构的特征中受益。其中一个关键的技术问题是要使得 RFID 读取器的无线功能起作用，允许它们与 WSN 的路由器进行通信，然后通过这些路由器把从 RFID 标签收集到的信息发送到服务器。解决这个技术问题最简单的方法是在硬件级别上集成无线路由器和 RFID 读取器。基于 ZigBee 的 RFID/WSN 体系结构如图 11.6 所示，其中一个有源 RFID 读取器和一个无源 RFID 读取器作为一个“有源 Zigbee 读取器”和“无源 Zigbee 读取器”。这两个 Zigbee 读取器可以与普通的 Zigbee 路由器进行通信，并形成 Zigbee 无线网络的骨干网。无线传感器节点只和它们的父路由器进行通信，有源标签和无源标签分别和它们的有源 Zigbee 读取器和无源 Zigbee 读取器相互通信。

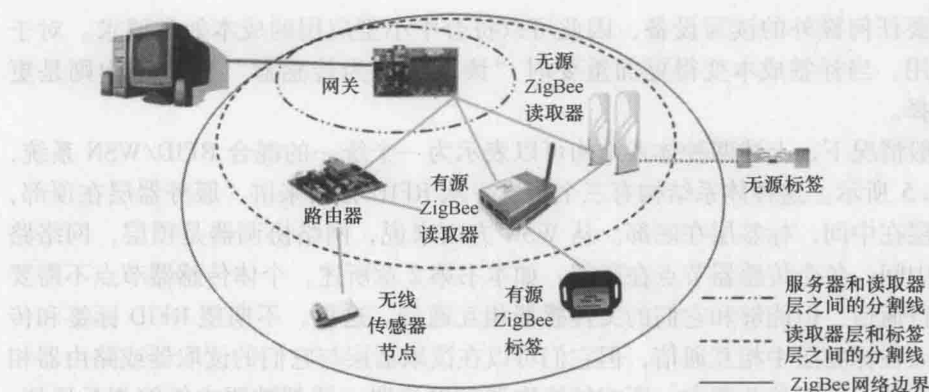


图 11.6 基于 ZigBee 的 RFID/WSN 体系结构（Yang 等，2011）

11.5 人道救援物流管理可行方案

人道主义援助的定义是“提供用于人道主义目的的物资或后勤援助”，通常应对人道主义危机。人道主义援助的主要目的是挽救生命、减轻痛苦、维护人的尊严。人道主义物流是一个广义的术语，涵盖了关于供应链策略、流程和技术，这将有助于使人道主义援助更有加效。

紧急援助物资的运输和交付是人道主义供应链的主要任务。因此，这类物资的初始运输是现场需要管理的首要问题。为了准确、有效地监控物资的流动，在物流中心里，如种类、数量、位置和状态的货物信息应进行记录和实时更新。食品和药品是人道主义供应链的主要物资，这些物资需在特定的环境条件下贮存和运输，这意味着环境监测信息也是必要的。其他的物资包括大型和有价值的特种救援设备（Özdamar 等，2004），如叉车、成套装置和车辆，也应进行跟踪管理和安全方面的考虑。因为灾害管理涉及受灾区域内的各种工作，所以在一个未知的环境里对设备和人员的定位跟踪是非常重要的人道主义援助行动。

总之，人道主义供应链中的配送中心对其信息支持系统有如下需求：

- 标识和识别不同类型的货物，并对物流进行跟踪；
- 监控部分货物的特定贮藏条件，从而保持其质量；
- 标识和识别如特种救援设备、车辆、机器和医疗设备等设备，出于物流和安全考虑还要对它们进行跟踪；
- 标识和识别员工及管理人员在中心的工作和生活情况，出于管理和安全考虑还要对他们进行跟踪；
- 拥有一个简单、可靠的网络体系结构和设备，不依赖任何在灾区不能保证的本地设施；

● 拥有一个简单、快捷的应急响应实施过程。

基于 ZigBee 的 RFID 传感器网络的人道主义物流中心如图 11.7 所示，人道主义物流中心实现了前文提出的集成混合 RFID 传感器网络体系结构。由于标准无源标签工作在金属和水这类物质的环境下性能很差，故有源标签被推荐用于跟踪场景中的车辆、工程成套装置、大型特种救援设备及人员等。ZigBee 终端设备被修改用作有源 RFID 标签；它们出于不同的目的可以被制造成不同的包装形式。为了跟踪中心的职员和官员，标签可制成腕带、徽章或者集成到其他如手表和移动电话等个人设备上。为车辆和设备包装用的有源标签可以带有皮带或螺钉孔，以便将它们安装在车辆底盘或设备架上。

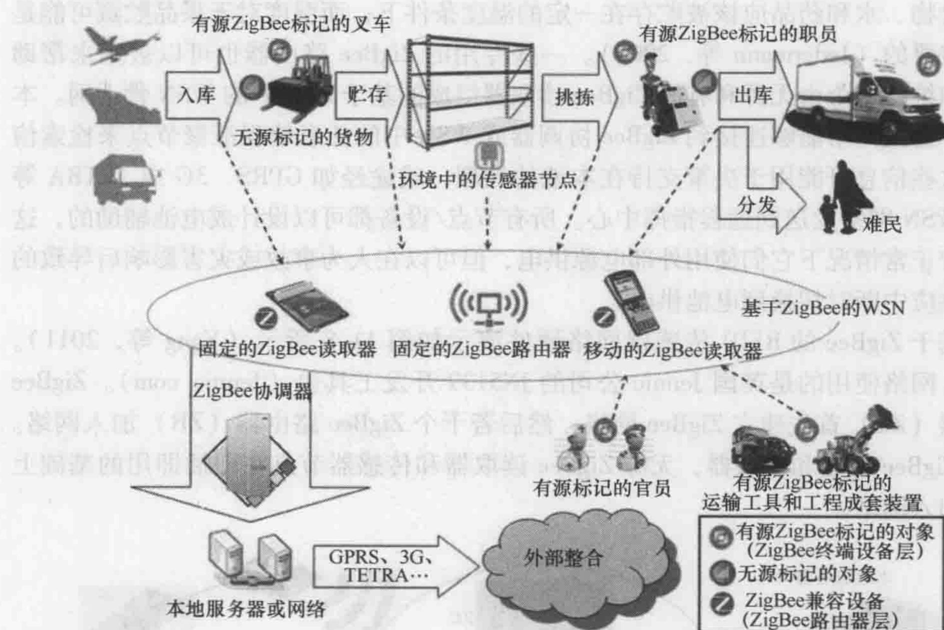


图 11.7　基于 ZigBee 的 RFID 传感器网络的人道主义物流中心（Yang 等，2011）

那些有源的 Zigbee 标签是与由典型的 ZigBee 路由器改成的有源 Zigbee 读取器进行通信的。这些读取器/路由器设备应部署在整个场景中，以确保覆盖整个中心。读取器的密度取决于安全级别或跟踪需要的精度。一般来说，可以分为三个层次：位置层、扇区层和房间。位置层的精度意味着需要跟踪对象的信息仅是它是否在岗位，这只需要基本数量的读取器来确保网络覆盖就可以了。这样的精度等级可以很容易满足，只要当标签在配送中心时可以与至少一个读取器/路由器设备进行通信即可。如果选择的是扇区层的精度，则要求每个标签都应该能够发现配送中心内的多个读取器/路由器设备。通过读取器的指示，该读取器是带有标签的具有最好的 RSSI，被跟踪对象的位置可以被限制在一个紧靠某个特定读取器的粗略区域内。在

某些需要房间级甚至米级精度的情况下，要求只要标签在配送中心，它就应该能够从不少于三个读取器/路由器设备得到 RSSI 或 TDOA 指示，因此需要最高的读取器密度。

经过配送中心的货物预计由典型的无源 RFID 标签来跟踪。传统的无源 RFID 读取器与 ZigBee 的路由器/读取器集成在一起，能够读取传统的无源标签和有源 ZigBee 标签。这些混合 ZigBee 读取器应该被安装在物流操作进行的所有接入点。

为了提高系统的灵活性，有源 ZigBee 读取器和无源混合读取器都可以被设计成带有充电电池的手持式设备，用于代替固定式读取器不可用时的临时操作。

专用的无线传感器节点还能够被部署在特定环境条件需要被监测的环境下。例如，食物、水和药品应该被贮存在一定的温度条件下；而湿度对于果品贮藏可能是至关重要的（Jedermann 等，2006）。一些专用的 ZigBee 路由器也可以被用来帮助建立和维持一个由无源和有源 ZigBee 读取器组成的基于 ZigBee 的 WSN 骨干网。本地服务器或网络能够连接到 ZigBee 协调器或 WSN 中的任意编程汇聚节点来检索信息，这些信息可能用于决策支持在本地的处理，或途经如 GPRS、3G 或 TETRA 等其他 WSN 网络发送到远程指挥中心。所有节点/设备都可以设计成电池辅助的，这意味着正常情况下它们使用外部电源供电，但可以在人为事故或灾害影响后导致的电力供应中断时切换到电池供电。

基于 ZigBee 的 RFID 传感器网络硬件演示如图 11.8 所示（Yang 等，2011）。ZigBee 网络使用的是英国 Jennic 公司的 JN5139 开发工具包（Jennic. com）。ZigBee 协调器（ZC）首先建立 ZigBee 网络；然后若干个 ZigBee 路由器（ZR）加入网络。有源 ZigBee 标签和读取器，无源 ZigBee 读取器和传感器节点在即插即用的基础上随后加入网络。

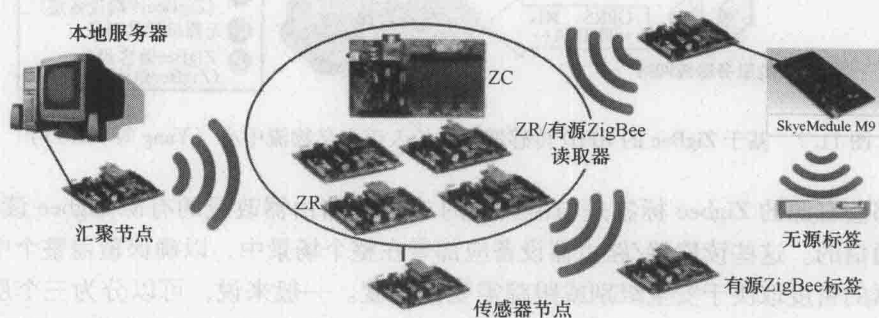


图 11.8　基于 ZigBee 的 RFID 传感器网络硬件演示（Yang 等，2011）

11.6　小结

许多专用系统目前都是为完成单个任务而存在的，如使用无源 RFID 识别货

物、WSN 用于监测环境及使用有源 RFID 跟踪人员和设备。但是没有一个系统可以同时处理所有这些任务。几个独立系统的实施和将它们集成到一个单一的软件/管理协调系统可能会导致应用中的各种问题。该混合 RFID/传感器网络提供了一个整合 WSN 的系统，无源和有源 RFID 共同位于硬件和软件层。它有一个统一的全面集成和无线的体系结构。本章介绍了这种类型混合网络的实现方式和可能的体系结构。提出“读取器作为传感器”和“标签作为传感器”两个概念作为混合 RFID/传感器网络的基础。关键是把 RFID 读取器与无线路由器集成并组成一个读取器/路由器网络。RFID 标签和无线终端设备能够同它们的读取器或路由器通信。并且，要求标签和无线终端设备之间不能相互通信。人道主义物流管理的可行应用为本章的研究案例。

参考文献

Englund, C., Wallin, H.: RFID in Wireless Sensor Network. Chalmers University of Technology Report, GÄoteborg, Sweden, EX034/2004 (2004)

Jedermann, R., Behrens, C., Westphal, D., Lang, W.: Applying autonomous sensor systems in logistics-combining sensor networks, RFIDs and software agents. Sens. Actuators, A **132**(1), 370–375 (2006)

Mason, A., Show, A., Welsby, T.: RFID and wireless sensor network integration for intelligent asset tracking systems. 2nd GERI Annual Research Symposium GARS-2006, Liverpool, UK (2006)

Özdamar, L., Ekinci, E., Küçükyazici, B.: Emergency logistics planning in natural disasters. Ann. Oper. Res. **129**(1–4), 217–245 (2004)

Pradhan, S.: RFID and Sensing in the Supply Chain: Challenges and Opportunities. HP Laboratories Tech Report HPL-2005–16 (2005)

Yang, H., Yang, L., Yang, S.H.: Hybrid Zigbee RFID sensor network for humanitarian logistics centre management. J. Netw. Comput. Appl. **34**(3), 938–948 (2011)

Yang, H., Yang, S.H.: RFID sensor network–network architecture to integrate RFID, sensor and WSN. Measur. Control **40**, 56–59 (2007)

第12章 物 联 网

关键词： 物联网 面向服务架构（Service-Oriented Architecture，SOA） 应急响应

12.1 引言

物联网（Internet of Things IoT）的概念是指物物相连的互联网，它提供了一个视角，使因特网延伸至真实世界，包括了日常的所有物体（Matter 和 Floerkemeier，2010）。术语“Internet of Things”因为美国麻省理工学院（Massachusetts Institute of Technology，MIT）的 Auto-ID 中心的研究工作而得到普及。1999 年美国 MIT 的 Auto-ID 中心开始设计和推广跨公司的 RFID 技术架构（Sarma 等，2000）。物联网的定义之一将其描述为“一个具有标准和互通信协议的自配置动态全球网络体系，协议规定物理的和虚拟的‘事物’都具有标识、物理属性和虚拟特性，并能够无缝集成到信息体系”（European Commission，2009）。图 12.1 给出了真实物理世界、虚拟网络世界和数字世界之间的相互作用。

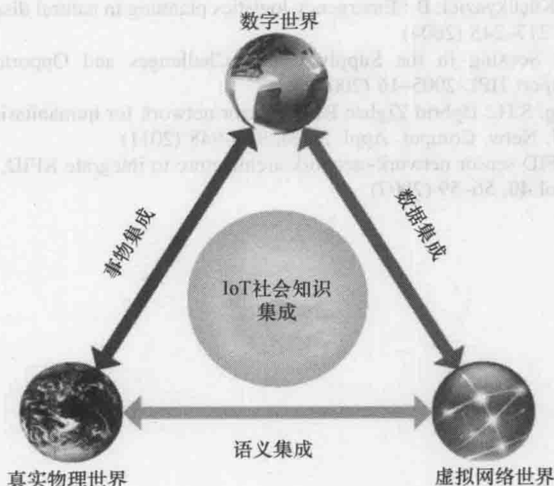


图 12.1 真实物理世界、虚拟网络世界和数字世界之间的相互作用（European Commission，2009）

网络设备中“物”的概念是指任何真实的或是虚拟的参与者，如现实世界的物品、人类、虚拟数据及智能软件代理。IoT 的目的是创造一个环境，任何来自连

接到网络的参与者的信息都可以实时地与其他参与者进行有效共享。在IoT研究和相关产业界中有很多“互联网”的定义。这些定义可能来源于单词“Internet”，导致“面向互联网”的研究视角；或来源于单词“things”，导致“面向物质”的视角。将“Internet”和“things”语义上结合起来，IoT是基于标准通信协议的可唯一寻址的互联物的全球网络。Atzori等人（2010）提出“面向语义”IoT的第三研究视角，并对IoT定义进行修改覆盖了这三个研究视角。来自欧洲委员会（2009）的研究路线图认为IoT是未来因特网的集成。一些研究者倾向于认为IoT是因特网的一个独立部分。Gershenfeld等人（2004）描述IoT是因特网的延伸，延伸至只支持低端计算机的地方和物理世界，而Fleisch（2010）认为IoT与因特网不是位于同一层次上的，事实上IoT是因特网的应用，就像很多现有的基于因特网的服务。

自从2005年IoT的概念提出以来，已经看到了为许多应用开发的基于网络的具有通信、感觉和行动能力的智能物体的配置，如卫生保健领域（Niyato等，2009）、智能建筑（Gill等，2012）、社交网络（Welbourne等，2009）、环境监测（Llic等，2009）、运输物流（Yang等，2011）等。所有的IoT应用都依赖从基于网络的分布式智能对象上采集的数据，即为数据传输服务的WSN和IoT信息基础设施。

12.2 物联网的特征与挑战

IoT的概念主要是由无处不在的计算机信息处理技术领域中不断进步的微电子技术和网络技术驱动产生的。它是一个涉及硬件、近场通信、网络、数据融合和软件工程等的多学科研究领域。在科学与技术方面的挑战需要它具有不同的能力（Association Instituts Carnot，2011）：

- 技术层。在强大的能源和环境约束下，这类挑战与智能网络对象的集成相关。
- 通信和网络层。这类挑战与大规模安全、动态、灵活的网络和无处不在的服务提供相关。
- 智能层。这类挑战与数据融合和服务发现相关，由各个智能网络对象（如RFID和无线传感器）收集的数据被分布式用户查询。

IoT中具有挑战性的三大领域如图12.2所示，涉及了IoT不同层次的技术结构。在技术层次上的关键功能是能够使“物”与“物”之间能够相互作用，即识别、传感、存储、执行及其他相互作用。现实世界和数字世界之间的连接要求数字世界有能力去感知现实世界并采取相应行动。一些如RFID、传感器、WSN等技术都提供本身特定功能支持IoT。然而，简单地装备微型芯片、在本地层次获取信息本身是不够的。这些IoT的智能网络对象超越了基于“简单”的传感器和RFID或

这两项的任意组合的现有设备。特别是，它们是基于廉价的小型无线设备，具有传感、执行、通信、先进的信号和信息处理能力。IP 技术如 6LoWPAN（IETF，2007），使构建低成本和可靠的解决方案和服务成为可能，这使得大量 IoT 中的“物”相互关联。



图 12.2 IoT 中具有挑战性的三大领域

IoT 的基本特征概括如下（Yang 等，2013）：

- IoT 是全球性的实时的解决方案；
- IoT 主要是面向无线的，能够提供室内和室外周边环境的全面数据；
- IoT 具有远程监控环境和跟踪或追踪物体的能力。

IoT 技术的第一个基本特征是，它是全球性的实时的解决方案。首先，IoT 技术是基于因特网或其他广域网的。因此，IoT 的范畴没有物理边界。任何连接至网络的对象都可以并入 IoT 中。其次，在 IoT 中数据通信是实时的或是接近实时的。从这个意义上说，它是有别于传统的数据库或 Web 系统的。

IoT 的第二个特征是，它是无线的，可以提供关于其周边环境的综合数据。IoT 中的 RFID 传感器网络整合了 RFID 网络和 WSN 成为统一的信息系统。RFID 传感器网络的传感任务无须在可视范围。此功能显著提高了信息的丰富度。

IoT 的第三个特点是，具有检测环境和跟踪物体的能力。通过 RFID 传感器网络和其他技术的结合，如 GPS 或红外传感器检测技术，RFID 传感器网络提供了无线、实时监测及跟踪任何被标记的室内或室外环境物体的功能，以便能够提供资源的完全可视性。这种可视性能够及时响应任何异常事件，在多组织、多用户和资源分配中进行分布式信息共享。

12.3 无线传感器网络与因特网连接

无论采取哪种定义，IoT 的核心需求是提供直接或间接地与网络上任意时刻来

自任何地方的智能“物体”的连接。比较因特网的定义——“连接在任何时间来自任何地点的任意一台计算机”，IoT 和因特网唯一的差别是在终端设备上，IoT 的终端设备是智能物体而不是计算机。WSN 是智能物体的网络。WSN 和因特网互联将形成 IoT 信息设施基础。

WSN 同因特网互联有很多方式（Kosanovic 和 Stojcev，2011）。从通信架构角度，Xu（2013）将互联方式分为三种，如图 12.3 所示。第一种方式为前端代理解决方案，通过中间件代理进行互联，WSN 和因特网之间并没有直接连接。第二种方式为网关解决方案，网关位于 WSN 和因特网之间。最后一种方式为 TCP/IP 覆盖解决方案，在 WSN 或因特网上构建一个重叠网络。下面进行详细叙述。

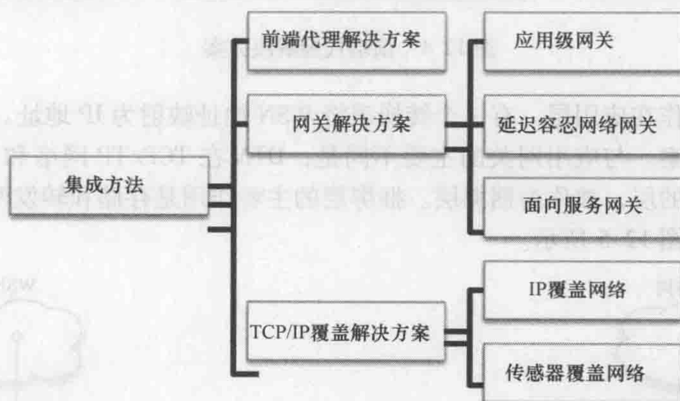


图 12.3　因特网和 WSN 集成分类

12.3.1　前端代理解决方案

如图 12.4 所示，TCP/IP 用户和传感器节点之间的通信是通过代理计算机完成的，而不是直接完成的。在传感器网络中使用的通信协议可以自由选择。代理主动收集来自 WSN 的信息并将其存储到数据库中。来自 TCP/IP 网络的用户可以通过多种渠道查询特定数据，如结构化查询语言或者基于 Web 的接口。其缺点是如果代理停止工作，所有的和 WSN 的往来通信全部中断，代理的实现通常依赖特定的任务或一组特定的协议。这意味着，每个应用程序都需要一个不同的代理。

12.3.2　网关解决方案

提供 WSN 和 TCP/IP 网络连接的基本设备之一是网关。它执行一些如协议转换、消息中继等方面的任务。因此，传感器节点和因特网主机之间就可以直接交换信息了。使用网关作为互联设备的所有解决方案，都可以被分为以下两类：应用网关和延迟容忍网络（Delay Tolerant Network，DTN）。应用网关是一个简单的基于网

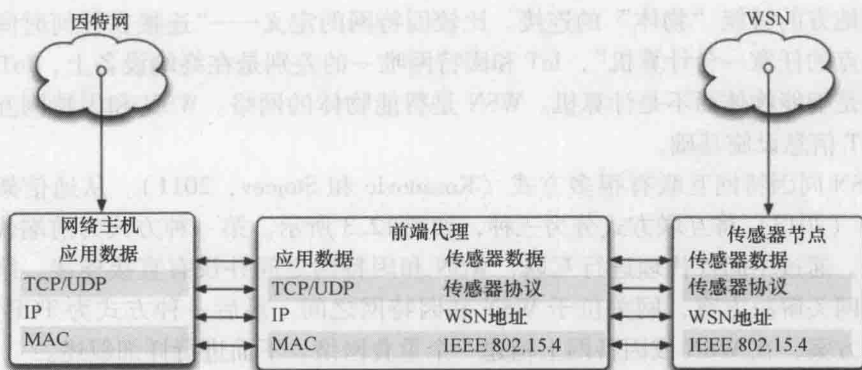


图 12.4　前端代理解决方案

关的方法，工作在应用层。有一个转换表将 WSN 地址映射为 IP 地址。DTN 是一个相近的解决方案。与应用网关的主要不同是，DTN 在 TCP/TP 网络和 WSN 网络中实现了一个新的层，被称为捆绑层。捆绑层的主要作用是存储和转发两个网络之间的数据包，如图 12.5 所示。

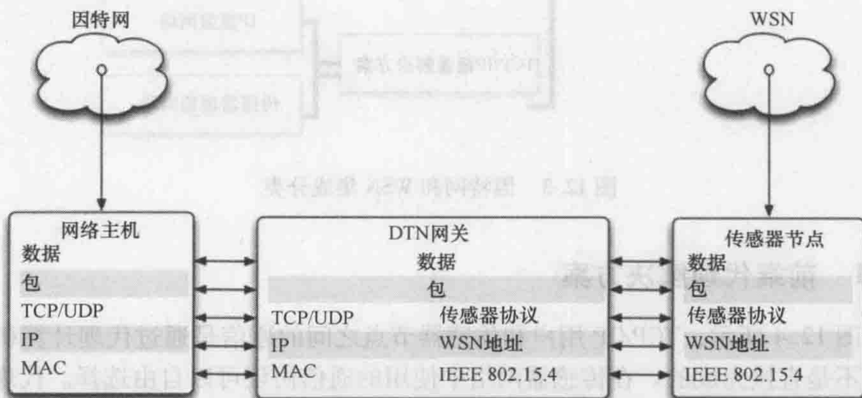


图 12.5　网关解决方案

12.3.3　TCP/IP 解决方案

TCP/IP 覆盖传感器网络是在资源非常有限的微型计算机系统上实现 TCP/IP 协议栈的，如图 12.6 所示。WSN 中的 TCP/IP 的实现相伴产生很多问题。例如，IP 地址是怎样分配给传感器节点的，以及如何根据网络流量有效地混合基于地址和基于数据的路由。6LowPAN 是一个典型的 TCP/IP 覆盖解决方案。它定义了在 IEEE 802.15.4 MAC 层上传输 IPV6 数据报的方法。因特网用户可以使用 IPV6 地址直接访问单个传感器节点。

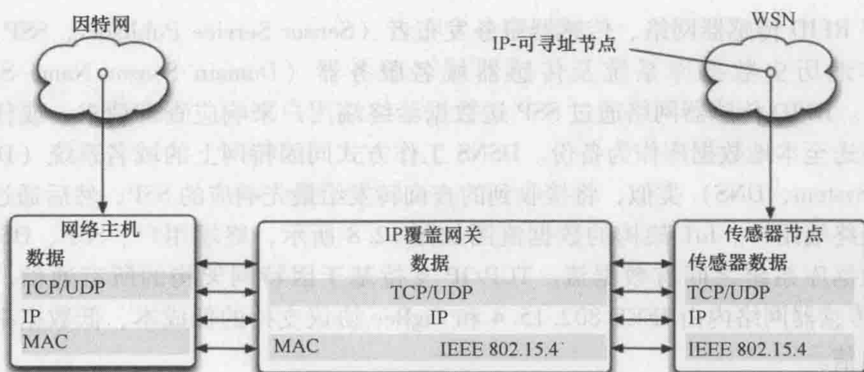


图 12.6 TCP/IP 覆盖解决方案

12.4 面向服务的物联网体系结构

面向服务的体系结构（Service-oriented Architecture，SOA）根据构架的三个主体，即服务生产者、服务消费者和服务注册，来定义信息架构。参与 SOA 的实体只有在单一交互时才受限只具有单一作用。服务生产者在一个或多个注册处发布它们的服务。服务消费者在注册处使用搜索工具查找需要的服务（Yang，2011）。

IoT 的 SOA 被设计成全球性地支持多用途、多应用和多数据源。它提供了一个统一的平台从分布式 RFID 传感器网络上收集、共享、处理和查询数据，并允许这些 RFID 传感器网络加入和离开 IoT，不影响系统其余部分。

实现这种方法的 IoT 体系结构，即 IoT 面向服务架构，如图 12.7 所示。主要的

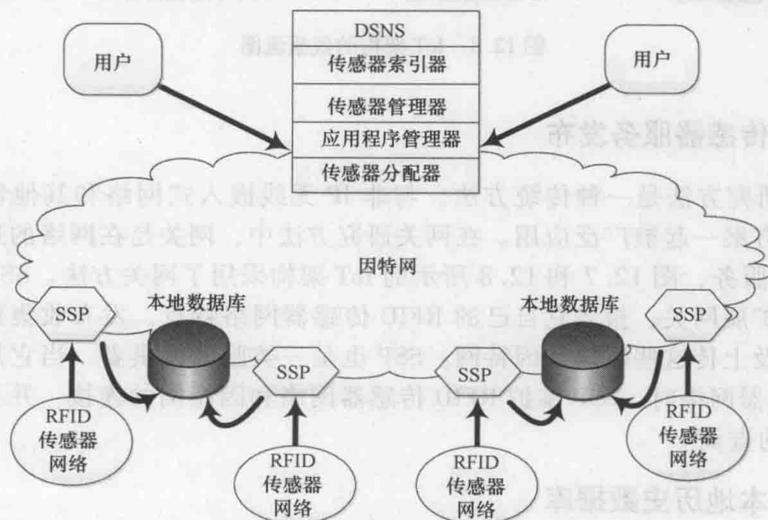


图 12.7 IoT 面向服务架构

组件有 RFID 传感器网络、传感器服务发布者（Sensor Service Publisher，SSP）、分布式本地历史数据库系统及传感器域名服务器（Domain Sensor Name Server，DSNS）。RFID 传感器网络通过 SSP 送数据给终端用户来响应查询请求，或任何变化时传送至本地数据库作为备份。DSNS 工作方式同因特网上的域名系统（Domain Name System，DNS）类似，将接收到的查询转发给最先响应的 SSP，然后通过因特网送至终端用户。IoT 架构的数据流图如图 12.8 所示，终端用户、SSP、DSNS 及本地数据库系统之间有数据流。TCP/IP 支持基于因特网架构的所有通信，除了 RFID 传感器网络内由 IEEE 802.15.4 和 ZigBee 协议支持的低成本、低数据率和短程的通信。

图 12.8 IoT 架构的数据流图

12.4.1 传感器服务发布

网关研究方法是一种传统方法，与非 IP 无线嵌入式网络和其他特定供应商的解决方案一起被广泛应用。在网关研究方法中，网关是在网络的边缘被引入处理 IP 服务，图 12.7 和 12.8 所示的 IoT 架构采用了网关方法。SSP 被设计作为一个扩展网关，报告它自己的 RFID 传感器网络特点，发布收集数据的可用性，以及上传这些数据到因特网。SSP 也是一类服务提供者。当它加入一个 RFID 传感器网络时，SSP 维护 RFID 传感器网络和因特网的连接，并且响应来自 DSNS 的查询。

12.4.2 本地历史数据库

在传统方法中，感知数据和其他信息被传输到服务器并被集中处理。然

而，集中处理有很多缺点。例如，集中处理的方法体现出信息及处理的能力不足、易于发生单点故障，并且在实时数据融合中有延迟等缺点。为了避免集中处理方法的这些缺点，分布式本地数据库被引入到每个已配置的 RFID 传感器网络。使用仓库作为实例，安装本地数据库用于存储数据变化，该数据由布置在仓库及仓库周围的 RFID 传感器网络收集而来，自动化的数据收集操作由仓库里的任何变化驱动和触发。终端用户可通过因特网查询数据，并直接通过 DSNS 到本地相应的数据库查询。对数据查询的响应是被本地数据库系统管理，并从本地数据库发送的。

12.4.3 传感器域名服务器

DSNS 是一种感知数据中央索引系统，工作方式与因特网上的域名服务器类似。DSNS 转发从终端用户接收到的查询给相应的 SSP 或相应的收集或存储查询数据的本地传感器数据库。查询响应形成后，结果就会发送给终端用户。DSNS 的特点是有一个传感器管理器、一个应用管理器、一个传感器索引器和一个传感器分配器。图 12.9 给出了 DSNS 组件间的交互和工作流程。其中，在线异常数据、离线异常数据分别流向终端用户和本地数据库系统，实时数据序列流向已标识的 RFID 传感器网络，历史数据序列流向已标识的本地数据库系统。

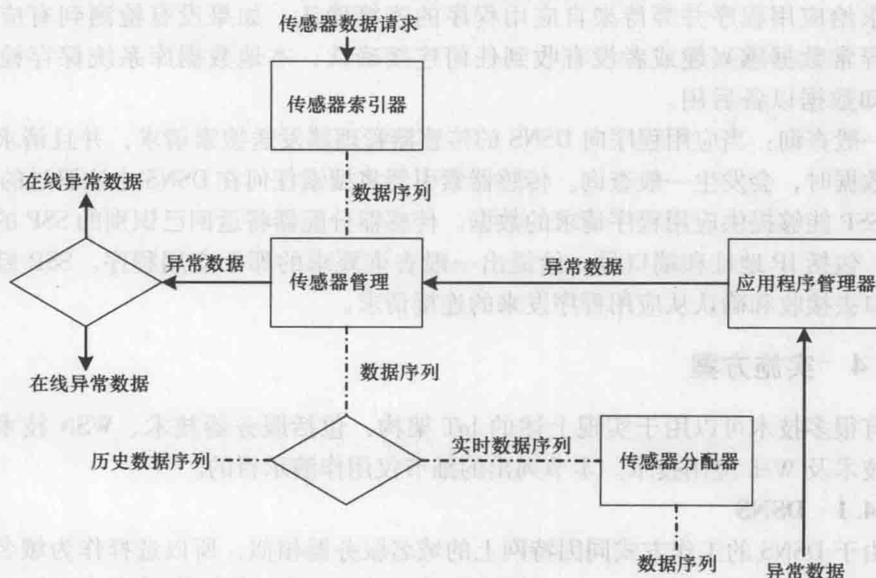


图 12.9 DSNS 组件间的交互和工作流程

● 传感器管理器用于传感器网络注册。它提供了一种通过指定的 RFID 传感器网络的类型、描述和名字来注册新的 RFID 传感器网络的机制。此外，它还提供了

一种更新先前已注册的 RFID 传感器网络特性的维护机制。

● 应用程序管理器用于注册应用程序信息，如 IP 地址、应用程序的功能及所需的感知数据的类型。存储这些信息的原因是为了当 RFID 传感器网络一旦捕获了预定义的异常数据时通知应用程序。

● 传感器索引器提供了一个搜索引擎，它根据传感器的类型和传感器的特点为注册的应用程序完成搜索服务。搜索引擎根据传感器的类型、位置和特征搜索 RFID 传感器网络。如果有一个或多个 RFID 传感器网络能够提供特定类型的感知数据，一个肯定的响应会被传送到传感器分配器，随后在已标识的 RFID 传感器网络和数据请求者之间的直接数据传输链路将被分配。

● 传感器分配器是 DSNS 中最重要、最大负载的部分。它分配数据请求者（即应用程序）和数据提供者（即 SSP）之间的连接链路。有两种类型的查询可能会触发传感器分配器：按需查询和一般查询。

按需查询：一旦 RFID 传感器网络检测到预定义异常数据，并且这些数据已经被传输到 SSP 时，会发生按需查询。SSP 将发布数据和收集数据传给 DSNS 的传感器的特性。DSNS 的应用程序管理器检查是否存在已注册的应用程序对检测到的异常数据感兴趣。如果有兴趣，应用程序管理器返回已识别的应用程序连接信息给传感器分配器。传感器分配器发送一个带有收听端口号的连接请求给应用程序并等待来自应用程序的连接确认。如果没有检测到有应用程序对异常数据感兴趣或者没有收到任何连接确认，本地数据库系统保存检测到的感知数据以备后用。

一般查询：当应用程序向 DSNS 的传感器管理器发送搜索请求，并且请求特定类型数据时，会发生一般查询。传感器索引器将搜索任何在 DSNS 中注册过的 SSP，这些 SSP 能够提供应用程序请求的数据。传感器分配器将返回已识别的 SSP 的详细信息，包括 IP 地址和端口号，给提出一般查询要求的那个应用程序。SSP 启动监听端口去接收和确认从应用程序发来的连接请求。

12.4.4 实施方案

有很多技术可以用于实现上述的 IoT 架构，包括服务器技术、WSN 技术，数据库技术及 Web 应用技术。本节列出的细节仅用作演示目的。

12.4.4.1 DSNS

由于 DSNS 的工作方式同因特网上的域名服务器相似，所以选择作为域名服务器基础的 SCO Unix（SCO Group，2010）作为实现 DSNS 的操作系统。SCO Unix 支持五种不同类型的配置，分别是主服务器、次服务器、高速缓存服务器、从属模式服务器及客户端。前 4 种模式与 DSNS 的特性相匹配，并已经被配置到构建 DSNS 中了。

12.4.4.2 SSP

SSP的职责包括感知数据的提取、DSNS中现有RFID传感器网络的注册及对DSNS中获取的控制命令进行应答。在ZigBee RFID传感器网络中，SSP作为一个具有IP功能的ZigBee路由来实现。它由两部分组成：一个是感知数据提取部分，即RFID传感器网络汇聚节点；另一个是服务发布和查询响应部分。感知数据提取部分收集需要的感知数据，并传输到服务发布和查询响应部分。这里完成数据读取、数据发布和服务控制。服务控制器存储所连接的RFID传感器网络的规范，由DSNS中的传感器分配器分配一个IP地址，以实现数据请求者的数据通信。

12.4.4.3 本地数据库系统

本地数据库系统使用MySQL实现，用于存储任何预定义的异常感知数据。它通过在DSNS上注册数据库服务器可以在因特网上使用。为了处理多数据查询，本地数据库系统引入了线程池的方法。线程池使得多线程可以及时使用。多任务重用线程能够减少线程创建的开销和响应时间。如果数据查询的数量达到事先预定的某一阈值时，本地数据库系统可以动态调节线程池中线程的数量。

12.4.4.4 终端用户应用程序

有两类终端用户应用程序，用于查询和消费由IoT架构提供的数据：单机应用程序及Web应用程序。单机应用程序是一个为大数据使用者服务的独立客户端，使用者需要定期检查感知数据，以及从固定RFID传感器网络中请求数据。可以采用Java编程实现跨平台的使用。Web应用程序是为只想快速浏览，但并不想或不需要事先在本地计算机上安装监测软件的用户提供服务的。Web应用程序包括一些基本功能，如登录、退出、搜索、登记各种需求及显示感知数据。它可以使用JSP或其他Web编程语言进行编码。终端用户，SSP及DSNS之间的通信协议使用TCP/IP。在SSP中，会采用IP功能的LR-WPAN协议，建立与因特网连接的上层链路，以及与RFID传感器网络连接的下层链路。

12.5 应急响应物联网的可行实现

当灾难来临时，第一响应小组不仅需要抢救和保护受灾地区的市民，他们还需要保持短期或长期的抵抗灾难的能力。物流组织工作一向被认为是应急操作中的重点因素。物流组织工作包括管理救援设备、交通工具、现场工作人员，以及食物、药品和一般生活品。应急响应需要大范围的组织参与，包括消防队、警察、救护车、地方或国家公共部门及如红十字会这样的人道主义援助组织。在分散组织之间的广泛的信息和资源共享是至关重要的，并且越来越普遍。图12.10给出了物流组织管理中IoT架构的实现。

灾区所有的救援设备、消防车、车辆、消防队伍、医疗工作者都贴上 RFID 标签。RFID 标签读取器被安放在通往灾区的入口。这些 RFID 读取器、标签和一些即时部署的环境传感器构成了 RFID 传感器网络。SSP 安装在配备有长距离无线通信设备，如连接了卫星或 WiMAX 网络的 3G 收发器的车辆上。靠近灾区的地方会建立一个或多个难民中心，那里的工作人员、食物、药品和日常生活用品也会被贴上标签。每一个难民中心形成了 RFID 传感器网络并且连接到 SSP，SSP 和远程 DSNS 或者终端用户可以通过卫星或是 WiMAX 网络进行通信。每一个 SSP 还安装了本地数据库系统。DSNS 可以安装在区域消防和救援服务总部，提供 IoT 架构的管理功能。通过 IoT 架构，消防总部、地方警察局及医院能够了解最新的灾情发展情况和响应进展。来自第一响应团队和难民中心的物流需求也要通知到相应的机构。

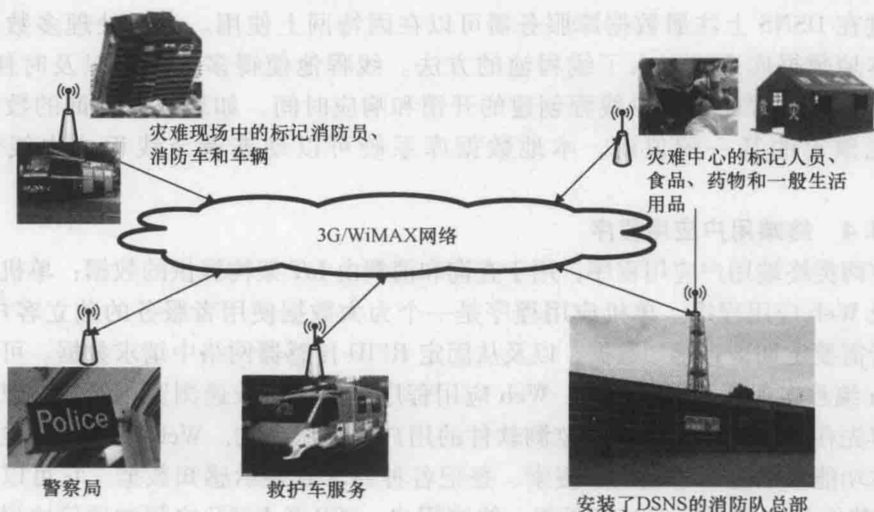


图 12.10　应急物流组织管理中 IoT 架构的实现（Xu 等，2013）

12.6　小结

本章提出了 IoT 的基本概念、特点、设计上的挑战，以及可能的体系结构。应急响应中可能的应用仅作为一个建设性的建议，有可能会被实现。

总之，IoT 应该被视为未来全部因特网的一部分，很可能同现在使用的因特网有惊人的不同。最大的区别在于，未来因特网或 IoT 的终端是连接着现实物品的传感器，而现在的因特网终端是个人计算机；未来因特网通过给每个 IoT 对象分配 IPv6 地址来访问单个物理设备，而现在的因特网仅被用作信息的检索与发布。因此，IoT 可能引爆因特网革命，使上述的发展趋势成为现实。

参考文献

Association Instituts Carnot: White paper: smart networked objects and internet of things, available online at http://www.instituts-carnot.eu/files/AiCarnot-White_Paper-Smart_Networked_Objects_and_Internet_of_Things.pdf (2011)

Atzori, L., Iera, A., Morabito, G.: The internet of things: a survey. Comput. Netw. **54**(15), 2787–2805 (2010)

European Commission: Internet of things strategic research roadmap, available online at, http://www.internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2009.pdf (2009)

Fleisch, E.: What is the Internet of Things? An economic perspective, Auto-ID Labs White Paper WP-BIZAPP-053, available online at, http://www.autoidlabs.org/uploads/media/AUTOIDLABS-WP-BIZAPP-53.pdf (2010)

Gershenfeld, N., Krikorian, R., Cohen, D.: The internet of things. Sci. Am. **291**(4), 76–81 (2004)

Gill, K., Yang, S.H., Wang, W.: A scheme for preventing low-level denial of service attacks on wireless sensor network based home automation systems. IET Wirel. Sens. Syst. **2**(4), 361–368 (2012)

IETF IPv6 over IEEE 802.15.4 low-power wireless personal-area-network, available online at http://www.6lowpan.org (2007)

Kosanovic, M.R., Stojcev, M.K.: Connecting wireless sensor networks to Internet. Facta Universitaties, Series: Mech. Eng. **9**(2), 169–182 (2011)

Llic, A., Staake, T., Fleisch, E.: Using sensor information to reduce the carbon footprint of perishable goods. IEEE Pervasive Comput. **8**(1), 22–29 (2009)

Mattern, F., Floerkemeier, C.: From the internet of computers to the internet of things. Informatik-Spektrum **33**(2), 107–121 (2010)

Niyato, D., Hossain, E., Camorlinga, S.: Remote patient monitoring service using heterogeneous wireless access networks: architecture and optimization. IEEE J. Sel. Areas Commun. **27**(4), 412–423 (2009)

Sarma, S., Brock, D.L., Ashton, K.: The Networked Physical World. TR MIT-AUTOID-WH-001 MIT Auto-ID Centre, Cambridge (2000)

SCO Group. SCO Official support document, available online at http://www.sco.com (2010)

Welbourne, E., Battle, L., Cole, G., Gould, K., Rector, K., Raymer, S., Balazinska, M., Borriello, G.: Building the internet of things using RFID: the RFID ecosystem experience. IEEE Internet Comput. **13**(3), 48–55 (2009)

Xu, R.: Federated sensor network architecture design for the IoT systems, Loughborough University PhD thesis (2013)

Xu, R., Yang, L., Yang, S.H.: Architecture Design of Internet of Things in Logistics Management for Emergency Response, IEEE International Conference on Internet of Things (iThings), pp. 395–402. Beijing, China, (2013)

Yang, H., Yang, L., Yang, S.H.: Hybrid Zigbee RFID sensor network for humanitarian logistics centre management. J. Netw. Comput. Appl. **34**(3), 938–948 (2011)

Yang, L., Yang, S.H., Plotnick, L.: How the Internet of Things technology enhances emergency response operations. Technol. Forecast. Soc. Change **80**(9), 1854–1867 (2013)

Yang, S.H.: Internet-based Control Systems. Springer, Berlin (2011)

第 13 章　基于 ZigBee 的智能家居系统：IndeedNet

关键字：家居自动化系统　节能　智能家居

13.1　引言

在诸多文献中都给出过有关家居自动化的定义。布罗姆利等人（2003）给出家居自动化定义：家居自动化是通过提供不同的服务，如远程医疗、多媒体娱乐和节能减排等，来提高居住者的生活质量的综合技术。

在家居自动化领域已经取得了显著的研究成果。例如 X10 行业标准，它始于 1975 年电子设备之间的通信，作者认为是最早的标准，它通过家居用电源线控制部分家电设备。近期，在家居自动化领域的研究持续受到学术界的关注。Al-Ali 和 Al-Rousan（2004）开发了一套基于 Java 技术的家居自动化系统，它采用嵌入式电路板物理连接所有家居自动化设备，并通过集成基于 PC 的 Web 服务器远程访问该系统。采用 Java 技术，结合内置的网络安全特性，实现了一种安全解决方案。但是，该系统需要内置式的昂贵的有线设备和高端 PC。Sriskanthan 等人（2002）提出基于蓝牙的家居自动化系统，包括一个主控制器和多个蓝牙子控制器。每个家用电器物理连接到一个本地蓝牙子控制器。家居设备使用有线方式与各自的子控制器通信，再从子控制器采用无线通信方式将所有通信信息发送到主控制器。理想状态是为每个家居设置都安装专用的蓝牙模块。然而，考虑到蓝牙设备的费用，单个蓝牙模块可以被多个设备所共享。通过使用无线技术，这种结构减少了所需的物理布线量并易于安装。Ardam 和 Coskun（1998）为家居和办公室自动化设计出一种基于电话的遥控器。该系统区别于前述系统之处在于所有通信都是基于固定的电话线，而不是基于因特网的。任何支持双音多频（Dual Tone Multiple Frequency，DTMF）的电话都可以接入该系统。该系统的缺点有三：不提供图形用户操作界面，使用者必须记住接入代码，需要记住每个按键对应哪个设备。

由大型企业提供的主要的家居自动化产品是 LG HomNet。该系统的核心是家居中的 PC，能控制如 LG 洗衣机、微波炉、空调、烤箱和冰箱等设备。英国的家居自动化产品包括英国电信（British Telecommunication，BT）的家居集线器和 Sky Multi-room（多空间）。BT 的家居集线器集成了高速互联网接入、无线个人区域网络和多媒体娱乐包（BT，2013）等功能。Sky Multi-room（多空间）包括多媒体网络，该包可分流 Sky 内容于家居的各个房间（Sky TV，2007）。

家居网关的开发试图为家居自动化系统提供网络互操作性和远程访问。Saito等人（2000）定义家居网关为“个人区域网络和公共接入网之间的接入点”。他们开发了一种基于Web服务器的家居网关，是基于电源线的家居自动化系统，通过IEEE 1394接口与因特网互联。Ok和Park（2006）提出一种基于开放服务网关初始化（Open Service Gate Initiative，OSGI）模型的家居网关，允许服务提供商通过访问家居自动化系统来管理和维护服务。该系统分为两个子系统。第一是数字家居服务的分发和管理系统（Distribution and Management System，DMS），提供了一个用户接口，用于控制和监测连接至家居自动化系统的设备。第二个是家居网关，负责管理家居自动化系统。对于一些用户来说，这种开放式的体系结构，可能更优于通过第三方所提供的隐私保护。

13.2　现有智能家居系统的分析

能被消费者采纳接受的家居自动化技术有限，被消费者广为采纳受限的原因分为五大类（Gill等，2009）。第一，复杂和昂贵的架构。现有的系统架构一般包括PC，以方便网络管理和提供远程访问。这增加了系统的复杂性，也因此增加了整体费用。第二，内嵌式安装。在某些情况下，因可选的无线技术的费用原因，大多数系统需要各类不同层次的物理布线结构。因此，这类系统需要内嵌式的昂贵的设备。第三，缺乏网络互操作性。家居网络和利用家居网络的家居自动化系统是以无计划和点对点（Ad-hoc）方式开发和采用的，这导致了家居网络环境变成复杂迷宫式异构网络。这些网络以及建立在其之上的系统通常提供很少的互操作性，导致以下三个潜在的问题：

- 由于缺乏互操作性导致重复监测活动；
- 共存网络间可能的干扰；
- 在共存网络内，两个同时存在而独立的行为相互作用可能导致一个并非期望的结果。

第四，接口缺乏灵活性。现有系统为用户提供了不同的方法来控制和监视所连接设备。然而，通常仅限于一个单独的控制方法，为用户提供有限的灵活性。提供多于一个接口设备的系统通常提供不同的用户界面，从而加大用户操作难度。第五，安全保障。现有的方法并没有重点关注来源于实施过程中的安全保障问题。此外，能够提供一定程度的安全等级的系统忽视了以建立安全为目的的多个设备厂商提供的设备间共享信息的问题。

13.3　智能家居系统体系结构

为了克服上述缺点，本节提出了一种新的独立的低成本基于ZigBee的灵活的

家居自动化系统。设计该结构的目标之一是减少系统的复杂度和降低费用。因此，系统努力尽可能不使用如高端 PC 等复杂昂贵的设备。该系统是灵活的可扩展的，允许由多个供应商设计的更多家电产品，以最小的代价安全可靠地加入到家居网络中。该系统允许房主监视和控制家中互联的设备，可使用各种控制方式，包括一个基于 ZigBee 遥控器，以及任何支持 Java 的具有 Wi-Fi 功能的设备。此外，用户可以监视和控制任何支持 Java 功能、具有因特网功能的设备。家居网关的实施是为方便异构网络之间的互操作性，并提供一个一致的界面，该界面独立于接入的设备。虚拟家居在真实的家居自动化系统启动之前预处理所有的通信。所有通信在发送至各自的目标前都要经过安全保障检测。

如图 13.1 所示，基于 ZigBee 的家居自动化系统主要包括四个步骤。远程用户可以通过因特网访问该系统。远程用户的通信跨越因特网直接到达家居网络。然后，通过家居 Wi-Fi 网络以无线方式传递到家居网关。家居网关与一个虚拟家居集成在一起。所有通信由家居网关和虚拟家居进行检查和处理，在后续章节中会有详细讨论。检查过程涉及与家居网络协调器之间的通信，该协调器与家居设备数据库集成在一起，并包含所有连接设备的状态。检测后，通信信息被发送到真实的家居自动化系统和各目的设备中。此外，使用基于本地 ZigBee 的遥控器可以直接控制连接的设备。

图 13.1 所示的家居网关负责为不同互联网络间提供互操作性。在该框架结构中家居网关提供两种主要的功能。首先，家居网关提供因特网、Wi-Fi 和 ZigBee 网络间的数据转换服务。其次，家居网关利用因特网远程连接或 Wi-Fi 本地连接为连接到 ZigBee 家居网络的设备提供了一个标准化用户界面。

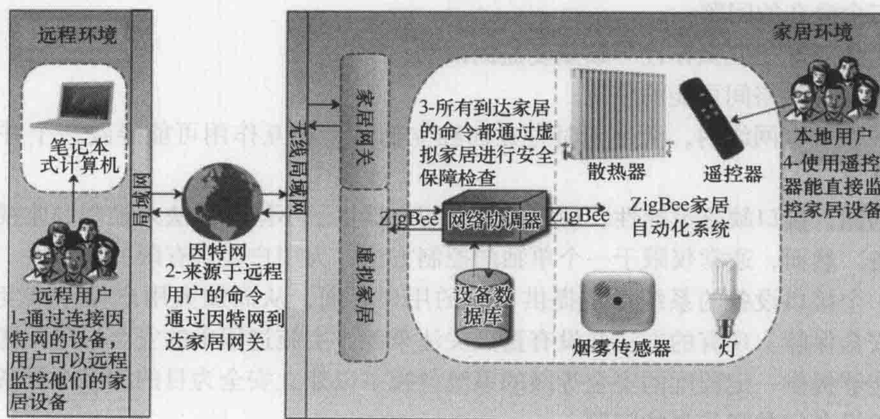


图 13.1 概念性总体框架结构

图 13.1 所示的虚拟家居负责家居自动化系统安全保障管理（Gill 等，2013）。虚拟家居，顾名思义，就是对用户请求操作进行检查的虚拟环境。出于安全考虑，

虚拟家居收到的所有消息都要经过认证发件人和消息完整性的检查，以确保它们没有被篡改，并要通过加密来保护信息。系统的安全性，是通过确保接收到的命令适合各自的家居网络，并且所有的改变请求在指定的安全限值之内，来保证的。虚拟家居主要目的是为了防止实施家居网络过程中任何事件带来的安全问题。

图 13.2 所示为基于 ZigBee 家居自动化系统。ZigBee 协调器负责建立和维护网络。系统中的每个电子设备（如洗衣机、电视机、灯泡等）均是由协调器管理的 ZigBee 设备。设备间的所有通信都通过协调器传播到达目标设备。ZigBee 的无线特性有助于克服早期家居自动化系统中内嵌设备的问题。理论上 ZigBee 标准提供 250 kbit/s 的数据速率。由于 40kbit/s 的速率就能满足大部分控制系统的要求，因此，ZigBee 足以控制大多数家居自动化设备。由 ZigBee 具有低安装成本和运行成本的优势，这有助于解决之前提出的现有家居自动化系统价格昂贵和架构复杂的问题。

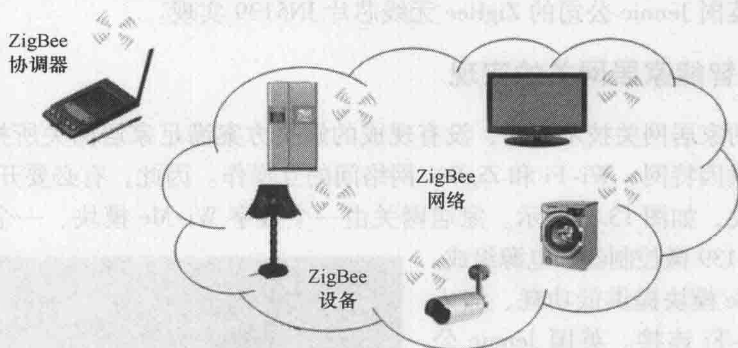


图 13.2　基于 ZigBee 的家居自动化系统

13.4　系统实现

13.4.1　基于 ZigBee 的智能家居系统的实现

ZigBee 家居自动化网络由一个协调器、多个路由器和若干终端设备组成。协调器负责初始化 ZigBee 网络。在网络初始化阶段，协调器将扫描可用的无线电信道，以找到最适合的一个。通常是选择最少活动的信道，以减少干扰程度。也可以限制指定信道的扫描，如不扫描共存于家居环境中 Wi-Fi 网络的频率范围。协调器对个人区域网络标识符（Personal Area Network Identifier，PAN ID）进行了预编程，所有连接到 ZigBee 家居自动化网络中的家居设备都被分配一个固定的 64 位 MAC 地址。此外，在一个网络生命周期内每个设备被分配了固定的动态 16 位短地址。在网络的初始化阶段，协调器分配给自身的短地址是 0x0000。初始化阶段之后，进入“协调模式”，监听 ZigBee 设备加入网络的请求。

家居网络 ZigBee 设备包括一个灯开关、一个散热器调节阀、一个安全传感器和一个 ZigBee 遥控器。一个 ZigBee 终端节点已经集成了这些设备。当设备被启动时，在其各自的初始化阶段，节点扫描可用的信道，以标识所希望加入的网络。同一个信道可能有多个网络，通常由它们的 PAN ID 区分。大部分 ZigBee 网络通过用户自定义的很短的允许设备加入的时间段，来防止未经授权的设备加入网络。在我们看来，就其本身而言这没有提供充足的网络安全性。为了提高系统安全性，我们提出系统加密所有设备通信，包括通过私有密钥请求加入家居网络。只有那些拥有正确私有密钥的设备可以成功连接到家居网络。被允许加入网络的设备都记录在设备数据库中，并存储在网络协调器内。ZigBee 家居自动化网络采用部分连接的网状拓扑结构。由于家居环境中通信干扰是不断波动的，所以增加通信路由是可行的，因为采用网状拓扑结构的优点可弥补所增加路由复杂性的缺陷。ZigBee 家居自动化网络采用英国 Jennic 公司的 ZigBee 无线芯片 JN5139 实现。

13.4.2 智能家居网关的实现

现有的家居网关技术表明，没有现成的解决方案满足家居网关所指定的功能。这包括提供因特网、Wi-Fi 和 ZigBee 网络间的互操作。因此，有必要开发一个定制的家居网关，如图 13.3 所示。家居网关由一个数字 Wi-Me 模块、一个英国 Jennic 公司的 JN5139 微控制器和电源组成。数字 Wi-Me 模块提供低功耗、嵌入式串行 Wi-Fi 连接。英国 Jennic 公司的微控制器提供与 ZigBee 网络的连接，数字模块连接到家居的本地 Wi-Fi 网络。英国 Jennic 公司的微控制器作为一个终端设备连接到 ZigBee 家居网络。

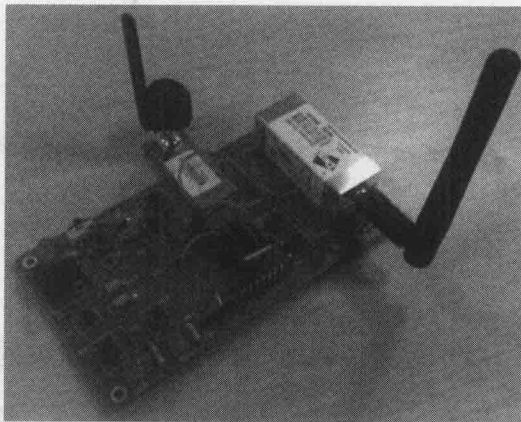


图 13.3　家居网关

家居网关一旦启动即进入配置阶段。在配置阶段嵌入式数字 Wi-Me 模块与本地 Wi-Fi 网络建立连接，如对网络 SSID 和安全参数等 Wi-Fi 连接参数进行预配置。同时，如先前所讨论的，英国 Jennic 公司的微控制器负责搜索 ZigBee 家居网络并建立连接。如同 Wi-Me 模块一样，Jennic 微控制器的连接参数被预先配置，这样就完成了配置阶段工作。

一旦家居网关被初始化后，即进入空闲状态，直到接收到输入数据。输入可以起始于 Wi-Fi 网络输入到 ZigBee 网络，或反过来从 ZigBee 网络输出到 Wi-Fi 网络。从 Wi-Fi 网络输入通常采用用户接口设备的命令形式。从 ZigBee 网络输入通常采用响应较早时接收到的来自用户接口设备的命令的形式。

13.4.3　虚拟家居的实现

虚拟家居是采用 C 语言实现的软件结构，在家居网关中实现。如图 13.4 所示，

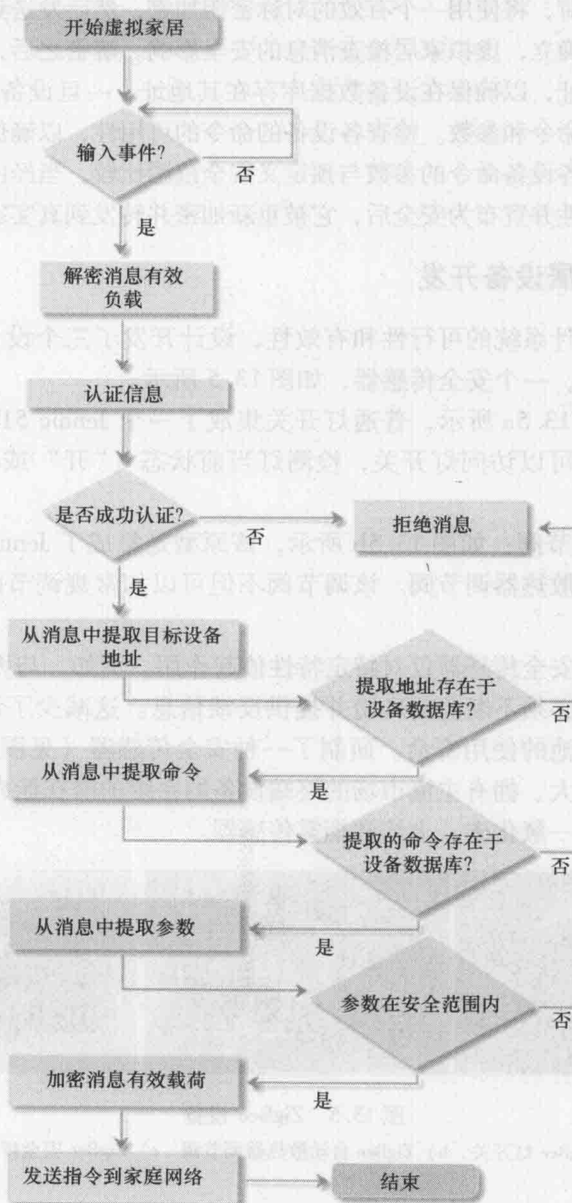


图 13.4　虚拟家居流程图

为了安全保障，在实施于真实家居环境之前，所有通信和指令都在虚拟环境中被检测。虚拟家居等待外部输入源。ZigBee 网络中所有设备集成 Jennic JN5139 微控制器和专用的 AES 协处理器。在家居网络中敏感信息被加密，因此，虚拟家居从合法来源获得消息的有效载荷，将使用一个有效的对称密钥加密，然后发送到家居网络。一旦消息的安全性已经确立，虚拟家居检查消息的安全影响。解密之后，从消息中提取和检查目标设备的地址，以确保在设备数据库存在其地址。一旦设备已存在于网络中，就可从消息中提取命令和参数。检查各设备的命令的可用性，以确保真实设备提供所要求的功能。提取各设备命令的参数与预定义安全范围比较，当经由虚拟家居算法验证消息的安全保障性并宣布为安全后，它被重新加密并转发到真实家居网络设备内。

13.4.4 智能家居设备开发

为了验证所设计系统的可行性和有效性，设计开发了三个设备：一个灯开关，一个散热器调节阀，一个安全传感器，如图 13.5 所示。

灯开关：如图 13.5a 所示，普通灯开关集成了一个 Jennic 5139 微控制器。在这个原型中，用户可以访问灯开关，检测灯当前状态（“开” 或 “关”），并可调整其相应的状态。

自动散热器调节阀：如图 13.5b 所示，该原型是集成了 Jennic 5139 微控制器而设计实现的自动散热器调节阀。该调节阀不但可以如常规调节阀一样手动控制，也可以远程监控。

安全传感器：安全传感器仅对特定特性值起作用。例如，与大多数安全传感器不同，安全传感器必须不断监测环境并提供反馈信息。这减少了设备的休眠时间，从而大大降低了电池的使用寿命。研制了一种安全传感器（见图 13.5c），旨在研究对系统资源需求大、拥有主流市场的终端设备的系统的潜在能力。已开发的安全传感器包含温度、一氧化碳、火焰和烟雾传感器。

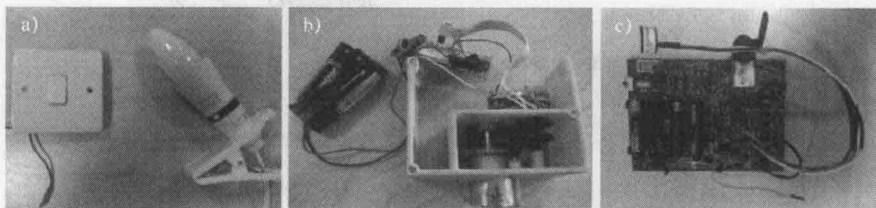


图 13.5 ZigBee 设备

a）ZigBee 灯开关 b）ZigBee 自动散热器调节阀 c）ZigBee 安全传感器

13.5 系统测评

家居自动化架构的可行性评估是通过实验室测试与散热器调节阀现场测试相结

合来完成的。对图 13.5b 所示的自动散热器调节阀进行了测试，测试地点位于图 13.6 所示测试房间地面。模型系统中自动散热器调节阀代替原有散热器 TRV 阀。

现场控制器采用无线方式连接到家居自动化系统，放置距散热器 2m 处。实验结果如图 13.7 所示，给出了以 30min 为周期的用户设定温度与实际测试温度比对结果。可以看出，该散热器的实际温度快速地调整到用户设定的温度。然而，实际的温度达不到 25℃。据推测，这是因为散热器太小而无法供热这么大的空间达到这个温度。

该实验表明，可以使用 ZigBee 通信标准，利用家居自动化系统，可成功监控散热器调节阀。成功的实验测评，显示出 ZigBee 智能家居系统的发展潜力，可以很容易地适应从实验室环境到商业市场的转换。

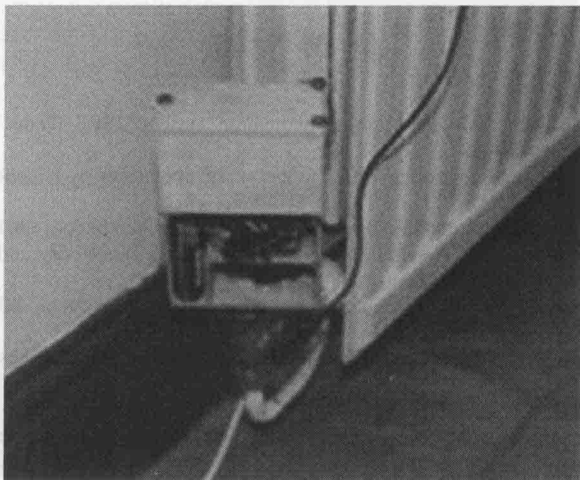


图 13.6　散热器调节阀现场

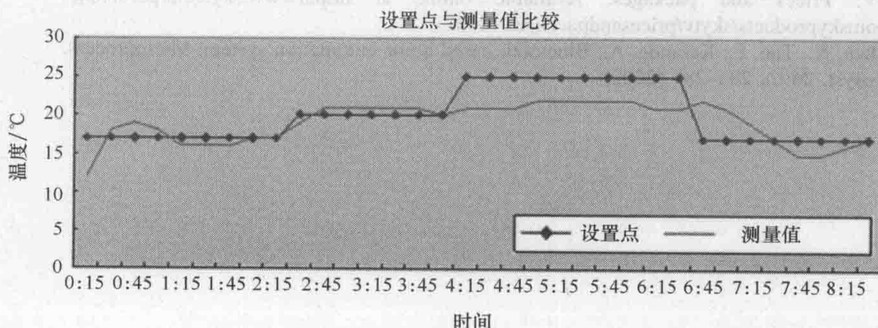


图 13.7　自动控制的室内温度实验结果

13.6 结论

本章评述了家居自动化系统的现状；并总结了阻碍消费者采用这项技术的五个问题：采用现有系统架构的复杂性和高成本，嵌入式系统安装问题，不同家居自动化技术之间缺乏互操作性，采用相同技术的不同厂商所开发系统之间缺乏互操作性、接口灵活性，以及对安全保障措施的不一致性问题。本章提出的 ZigBee 智能家居系统克服现有系统的弊端。采用 ZigBee 通信技术有助于降低系统成本和各系统安装的复杂性。虚拟家居概念的引入整合了清晰的和一致的系统安全保障措施。家居网关技术有助于解决网络间的互联互通问题，家居网关实现了本地 ZigBee、Wi-Fi 和因特网网络间的互操作。建立的一个低成本、灵活和安全的家居自动化系统体系结构，已通过实验室和现场测评，表明其是可行和适用的。

参考文献

Al-Ali, A.R., Al-Rousan, M.: Java-based home automation system. IEEE Trans. Consum. Electron. **50**(2), 498–504 (2004)

Ardam, H., Coskun, I.: A remote controller for home and office appliances by telephone. IEEE Trans. Consum. Electron. **44**(4), 1291–1297 (1998)

British Telecom: BT home hub. Available online at http://www.homehub.bt.com (2013)

Bromley, K., Perry, M., Webb, G.: Trends in smart home systems, connectivity and services. Available online at www.nextwave.org.uk (2003)

Gill, K., Yang, S.H., Yao, F., Lu, X.: A zigbee-based home automation system. IEEE Trans. Consum. Electron. **55**(2), 422–430 (2009)

Gill, K., Yang, S.H., Wang, W.: Secure remote access to home automation networks. IET Inf. Secur. **7**(2), 118–125 (2013)

LG HomNET: Solution models. Available online at http://global.dreamlg.com (2013)

Ok, S., Park, H.: Implementation of initial provisioning function for home gateway based on open service gateway initiative platform. In: Proceedings of the 8th International Conference on Advanced Communication Technology, pp. 1517–1520 (2006)

Saito, T., Tomoda, I., Takabatake, Y., Ami, J., Teramoto, K.: Home gateway architecture and its implementation. IEEE Int. Conf. Consum. Electron. 194–195 (2000)

Sky TV: Prices and packages. Available online at http://www.sky.com/portal/site/skycomskyproducts/skytv/pricesandpackages (2007)

Sriskanthan, N., Tan, F., Karande, A.: Bluetooth based home automation system. Microprocess. Microsyst. **26**(6), 281–289 (2002)

第 14 章　建筑物消防安全防护：SafetyNET

关键字：防火安全　ZigBee　建筑物环境监测

14.1　引言

火灾具有杀伤力。防止火灾就是拯救生命、减少伤害。另外，防止火灾也可以节省资金。所以，为了保护人们，把防止火灾发生摆在首位是具有重要意义的。以最有效的方式确保救火时的人员安全（Yang，2007）也是很有意义的。准确可靠的信息对有效应对突发事件是至关重要的。控制中心的工作人员根据事件的信息，对可用资源的配置做出关键性决策。第一响应者的部署也依靠这些信息来准备实际的应急预案。因此，突发事件信息的准确性和可靠性可能具有生死攸关的影响。

Yang 等人（2009）的研究表明，需要收集以下四类信息并在现场应急响应信息系统中共享和报告，不仅可以保证应急响应，同时也可以确保成功实施应急响应。

- 环境条件：当第一批响应者到达事故现场，他们拥有非常有限的环境信息，不知道建筑或者地铁站是否可以安全进入，以及如何最有效地应对灾害。许多一线救援人员可能会面临不熟悉的危险情况。决策者应该意识到这些危险的存在，并对环境条件有一个整体上的认识。然后，在他们派遣随后的救援人员之前，制订出一个处理灾难的方案。
- 参与者的信息：一些灾害情况涉及数以百计的来自不同组织机构的个人来合作应对事件。知道谁参与了响应、他们能提供什么能力、带来什么样的资源到现场，这些信息都将使事故指挥者能够以最有效和最佳协调方式做出决定、应对现场局面。
- 伤亡情况：响应事件期间，参与机构间获取和快速共享最新伤亡数据、报告事故地点、事故原因和严重程度，对确保参与者采取适当的抢救措施、迅速协调紧急医疗服务是至关重要的。
- 可用资源：一旦发生重大灾难，许多政府和非政府组织会将大量的设备和其他资源快速地运送到受灾地区。通常，对设备没能实现集中控制或存贮。收集和共享可用设备的信息，确保救援者从已经到达事故现场的大量设备中找到他们需要的设备是至关重要的。

14.2 系统架构

SafetyNET 提供了一个系统架构，使建筑物、消防队员、消防车和他们的控制中心，在发生自然的和人为的火灾事故时，通过使用传感器网络、无线通信、数字音频广播（Digital Audio Broadcasting，DAB）和陆上集群无线电（Terrestrial Trunked Radio，TETRA）技术等进行有效通信。系统架构由三层组成（Yang 和 Frederick，2006），如图 14.1 所示。

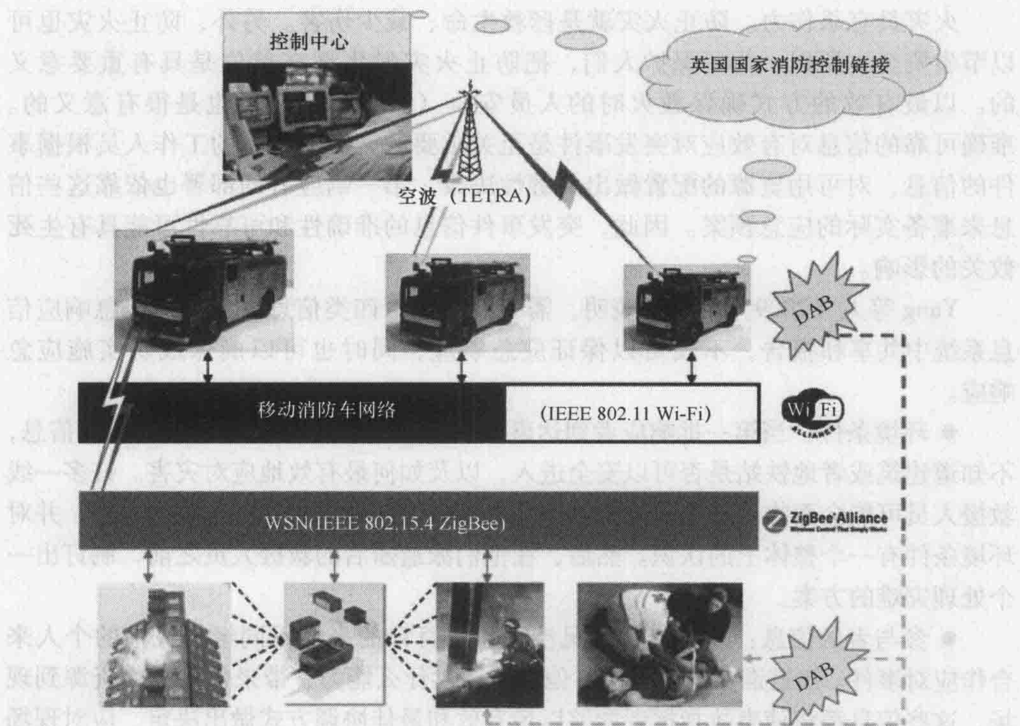


图 14.1 SafetyNET 系统的系统架构

底层包括安装在建筑内或在建筑物周围的一个健壮的 WSN。传感器网络利用健壮的传感器节点检测任意指定位置的任何环境变化。传感器网络可以代替现有的火警网络，这意味着先前安装的火警网络并不是必须要具备的。被收集到的信息流经传感器网络，然后传输至消防车网络中。

中间层包括安装在消防车上的车载移动网络。它是通过升级新推出的车载移动数据系统（Vehicle-mounted Mobile Date System，VMDS），增加上行链路到控制中心，增加下行链路到 WSN 来实现的。关于建筑物、住户和消防队员位置的实时信

息从传感器网络中收集、传输并提供给消防车网络。在消防车赶往事故现场的途中，与建筑物相关的最新信息，如平面图和消防栓状态，从控制中心的中央数据库下载到消防车网络。DAB 使用于底层和中间层之间，以便维护消防车网络和紧急救援人员之间的限时单向通信信道。

顶层是位于消防队控制中心的中央设备。控制中心的应急响应管理系统将提供给消防队员最新的关键信息、远程监控事件的最新发展。

14.3　SafetyNET 专用设备

一个典型的 SafetyNET 系统由四种类型的设备组成：一个 ZigBee 协调器，ZigBee 路由器，ZigBee 终端设备和 ZigBee 适配器。ZigBee 协调器是 SafetyNET 传感器网络的发起者和网络管理者，负责建立和维护网络。网络维护及采用的路由协议的功能是通过 ZigBee 的协议栈实现的。除了不建立网络以外，ZigBee 路由器类似 ZigBee 协调器。ZigBee 的路由器扩展了 SafetyNET 系统的覆盖面。它负责适应新的 ZigBee 终端设备连接到网络上，处理终端设备的离开请求，并实现路由协议。ZigBee 终端设备是 SafetyNET 的传感器节点，安装在环境状况可能改变的建筑物内，对建筑物安全是至关重要的。ZigBee 适配器是一个 ZigBee 设备，允许任何计算机访问 ZigBee 网络。图 14.2 给出了 ZigBee 适配器原型。它一边是与计算机连接的 USB 接口；另一边是访问 ZigBee 网络的 ZigBee 天线。图 14.3 总结了 SafetyNET 的 ZigBee 网络设备及功能。

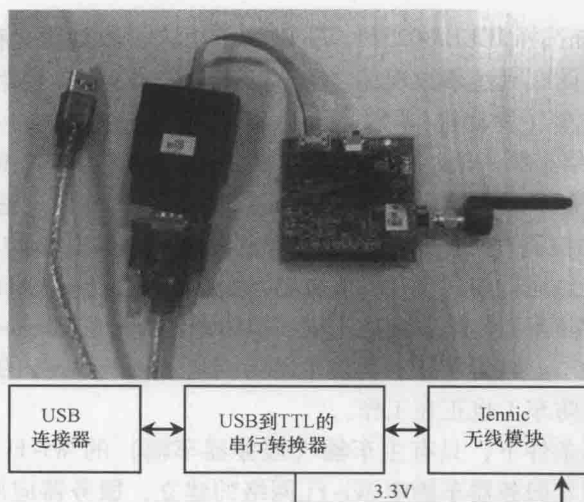


图 14.2　ZigBee 适配器原型

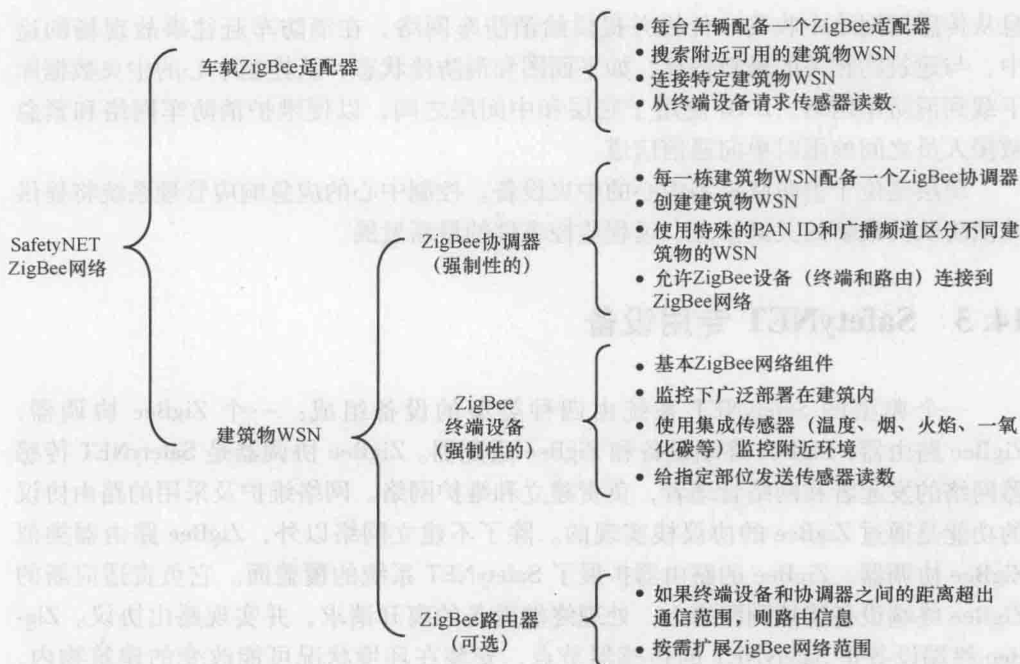


图 14.3　SafetyNET 的 ZigBee 网络设备及功能

14.4　移动消防车载网络

SafetyNET 系统选择 IEEE 802.11 Wi-Fi 通信协议，即刻构建移动消防车网络。实际上，在任何消防车到达事故现场之前移动消防车的 Wi-Fi 网络并不存在。只有当一个或几个消防车（发动机/车辆）到达现场，整个三层 SafetyNET 才能完全建立起来。Wi-Fi 网络是第一辆消防车（主车辆）到达现场通过其 Wi-Fi 协调器默认建立的，所以系统的启动是从 Wi-Fi 网络开始的。后续的车辆、适配器，通过它们的车载 Wi-Fi 自动检测并加入到已存在的 Wi-Fi 网络。移动消防车网络如图 14.4 所示，说明了在应急运行期间 Wi-Fi 服务器/数据库信息传输的原则。其中，消防车 1 是主车辆；消防车 2 是稍后到达车辆，消防车辆 2 中的 ZigBee 适配器和 Wi-Fi 协调器处于闲置状态。因为从移动消防车网络到建筑物的 WSN 的唯一下行链路由消防车 1 维护，消防车 1 也正在工作。

因此，在工作条件下，只有主车辆（服务器车辆）的 Wi-Fi 协调器和 ZigBee 适配器被激活。随着服务器车辆中 Wi-Fi 网络的建立，服务器应用程序从 WSN 中取回传感器数据，这些数据再通过装备在服务器车辆的 ZigBee 适配器存储到一个数据库中。然后，应用程序将这些数据信息共享到所有车载数据终端（计算机）

的Wi-Fi网络，并显示在一个基于Web的图形用户界面（Graphical User Interface，GUI）上。该信息每2~3s会自动更新一次。

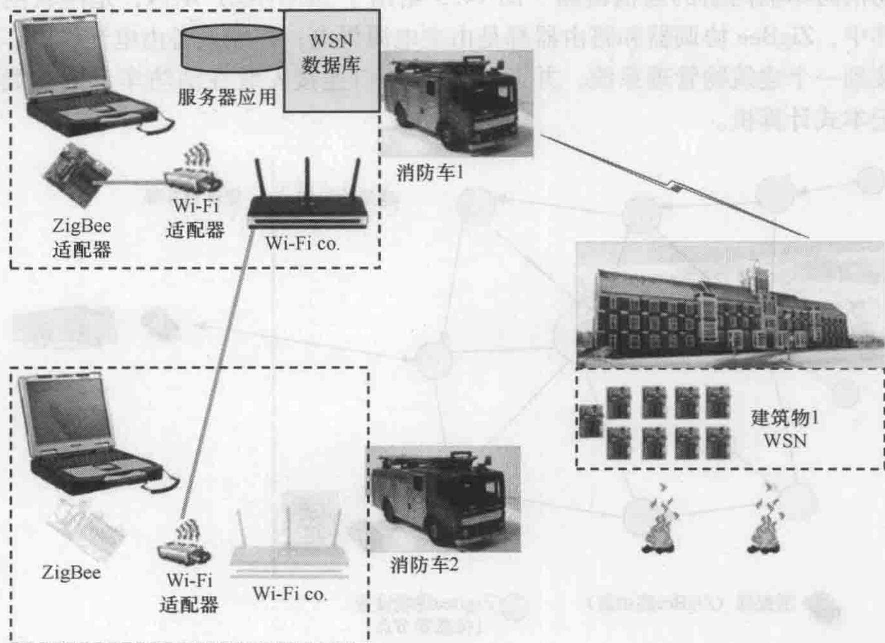


图14.4　移动消防车网络

有时候，某一台后续车辆（非主车辆或客户端车辆）需要成为新的主车辆（新的服务器车辆）；或者是因为它是一个后到达的命令单元，需要获得数据及数据库的控制权；或者是因为现有的主车辆因其他任务不得不离开现场。在这种情况下，确认无误后，潜在的主车辆的ZigBee适配器将被激活，服务器角色连同数据库一起从当前的主车辆转移给潜在的主车辆。最后，新的主车辆将开始使用它自己的ZigBee适配器从建筑物的WSN中获取传感器数据，并将信息共享到其他终端上。当然，新的数据将被追加到旧的已有数据库中，因此传感器数据始终以唯一的版本得到完整维护。先前的主车辆可能会离开现场；然后，新的主车辆的Wi-Fi协调器将自动重新建立一个新的Wi-Fi网络，几秒内就能继续信息共享。

14.5　SafetyNET无线传感器网络

如图14.3所示，SafetyNET WSN由SafetyNET协调器、路由器、终端设备和适配器组成。SafetyNET WSN位于图14.1所示的系统架构的底层。该SafetyNET协调

器和路由器形成一个基于 ZigBee 的网状网络，网络中各种终端设备连接它们的路由器，结果该网状网络可以感知任何环境条件下的变化。通过 ZigBee 适配器保持与移动消防车辆网络的通信链路。图 14.5 给出了 SafetyNET WSN，是网状网络架构。其中，ZigBee 协调器和路由器都是由主电源供电；终端设备由电池供电；适配器连接到一个建筑物管理系统，并通过 USB 端口连接安装在消防车上的功能强大的笔记本式计算机。

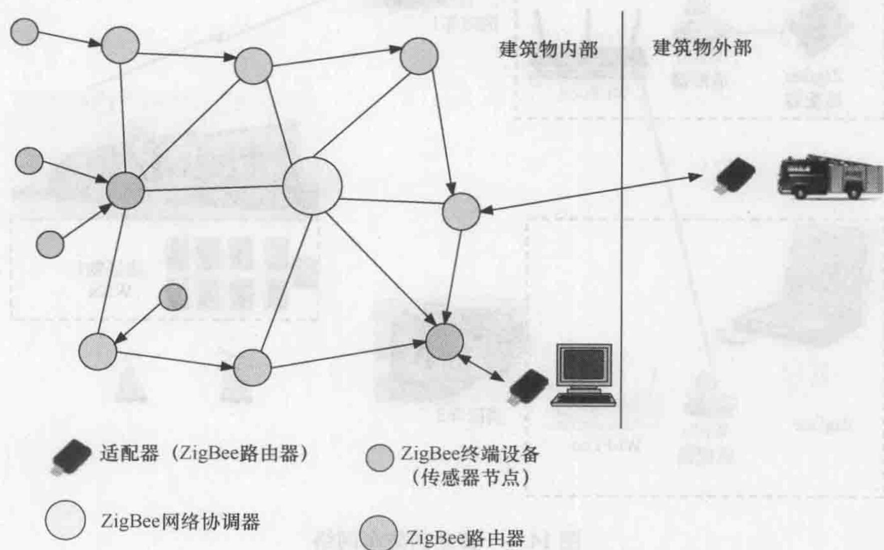


图 14.5　SafetyNET WSN

14.5.1　SafetyNET 协调器

该 SafetyNET 协调器是 ZigBee WSN 的启动者。它也是一台特殊的设备，能够在网络中起到 ZigBee 路由器的作用。协调器的作用主要包括网络初始化和网络维护。ZigBee 协议栈处理网络维护和路由协议的实现。图 14.6 给出了 SafetyNET 协调器的状态机。硬件初始化用于初始化安装协调器的外围设备，包括按钮、液晶显示器（Liquid Crystal Display，LCD）和发光二极管（Light Emitting Diode，LED）。这些外围设备可以用来支持与用户的交互操作。网络堆栈的初始化是设置网络的 PAN ID 和网络通道。网络冲突处理可能需要协调器来调整这两个参数。如果没有冲突或冲突已经解决，协调器就进入建立网络状态，并且它的 PAN ID 为 WSN 保留下来。这意味着，如果有其他 ZigBee 协调器接近 SafetyNET WSN，它们不能使用同一个 PAN ID。在网络维持状态下，协调器负责接收加入或离开由路由器设备所连接的网络的任何请求。

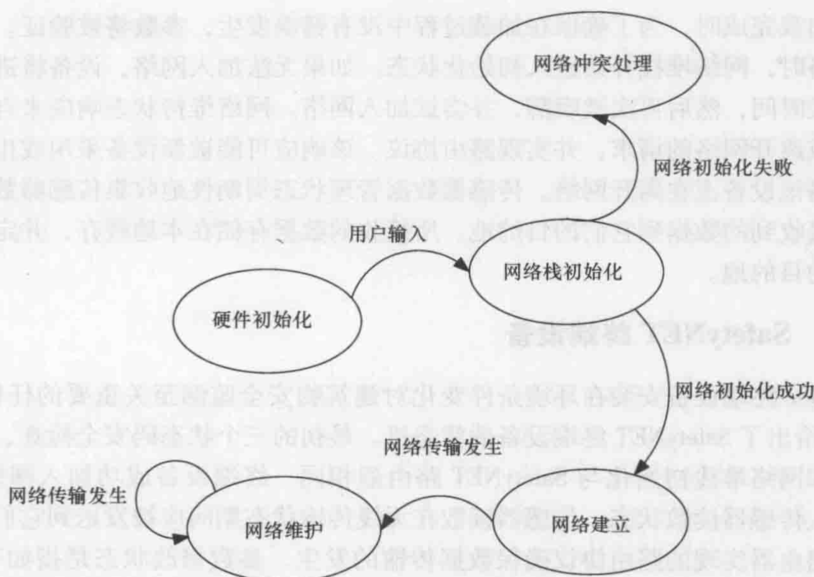


图 14.6　SafetyNET 协调器的状态机

14.5.2　SafetyNET 路由器

除了不能够创建网络外，SafetyNET 路由器执行的功能类似 SafetyNET 协调器。图 14.7 给出了 SafetyNET 路由器的状态机。代码安全检查是保护设备不被任何潜在的入侵者替换或修改。如果代码安全检查失败，设备将停止任何进一步的动作。参数初始化状态从板载内存（通常存储在 EEPROM）中加载自定义参数或默认参数。

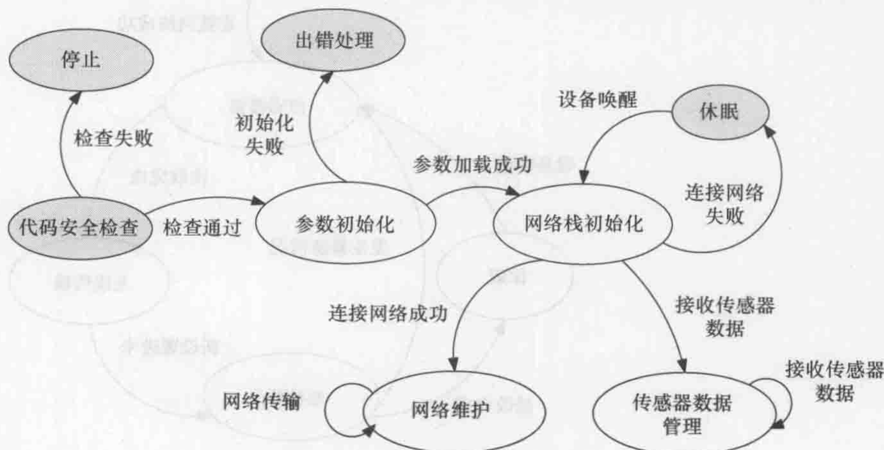


图 14.7　SafetyNET 路由器的状态机

当参数加载完成时，为了确保在加载过程中没有错误发生，参数将被验证。当设备加入网络时，网络堆栈开始进入初始化状态。如果无法加入网络，设备将进入休眠模式一段时间，然后再次被唤醒，并尝试加入网络。网络维持状态响应来自其他设备加入或离开网络的请求，并实现路由协议。该响应可能被新设备采用或拒绝，并通知网络该设备正在离开网络。传感器数据管理状态周期性地收集传感器数据，然后转发接收到的数据到它们的目的地。所接收的数据存储在本地缓存，并定期发送到它们的目的地。

14.5.3 SafetyNET 终端设备

ZigBee 终端设备安装在环境条件变化对建筑物安全监测至关重要的任何地方。图 14.8 给出了 SafetyNET 终端设备的状态机。最初的三个状态码安全检查、参数的初始化和网络堆栈初始化与 SafetyNET 路由器相同。终端设备成功加入网络之后，系统进入传感器读数状态。传感器读数在无线传输状态期间应被发送到它们的目的地。由路由器实现的路由协议确保数据传输的发生。参数修改状态是指如有必要，更新终端设备的参数。为了节约能源，SafetyNET 终端设备将进入休眠模式。网络

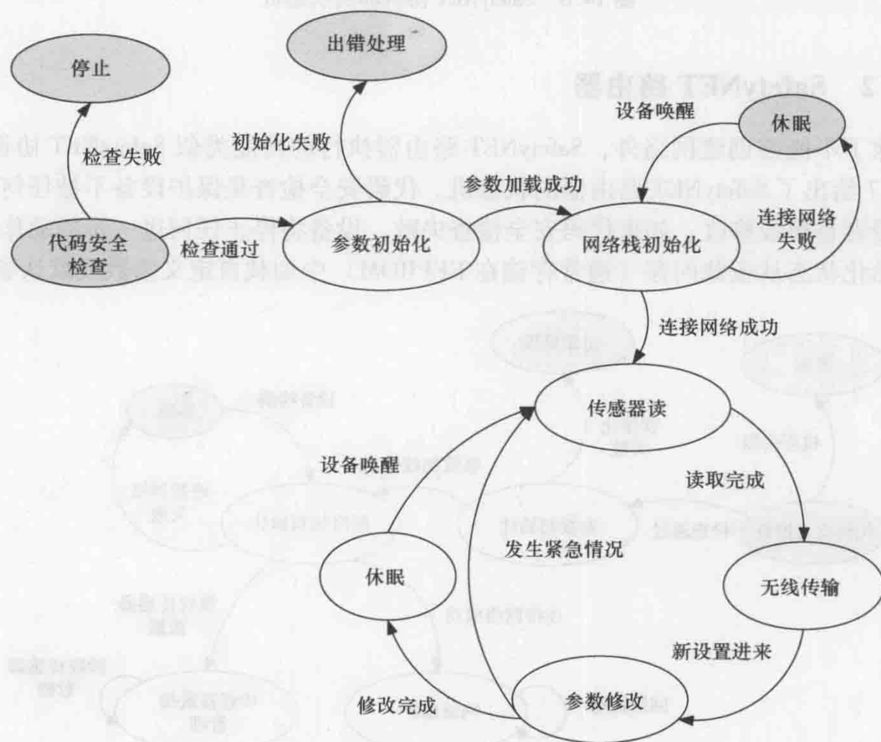


图 14.8 SafetyNET 终端设备的状态机

堆栈和内存的内容将在设备休眠之前被保存。当系统唤醒时，SafetyNET 终端设备将恢复内存，继续检测活动。在紧急情况下，休眠状态被绕过，参数修改状态之后紧接着进入传感读取状态。

14.5.4 SafetyNET 适配器

SafetyNET 适配器用于移动消防车访问 ZigBee 网络。图 14.9 给出了 SafetyNET 适配器的状态机。参数设置包括自动选择 SafetyNET WSN 的 PAN ID 和 IEEE 802.14 的信道。网络堆栈初始化状态与路由器及终端设备相同。加入 SafetyNET WSN 后，适配器充当消防车载网络和 SafetyNET WSN 之间的中介。

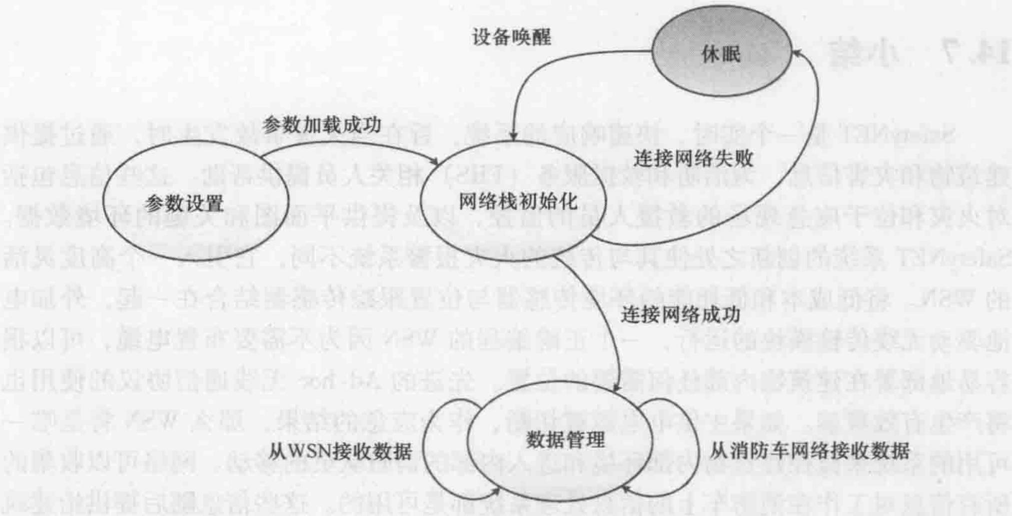


图 14.9 SafetyNET 适配器的状态机

14.6 现场试验

在本地的消防和救援服务培训中心进行了 SafetyNET 的现场实验。某房间发生火灾之前，SafetyNET 系统被部署在训练建筑物内部。图 14.10 所示为用于现场实验的培训建筑物及部署在其内的 SafetyNET 无线传感器节点。配备的一台超强笔记本式计算机和一个 ZigBee 适配器的消防车被无线连接到 SafetyNET WSN。现场试验结果表明，预期的环境数据信息、火场和消防队员的位置均能成功地通过位于建筑物外部的系统获得，而该建筑物的内部正发生火灾。使用 SafetyNET 系统，指挥官员可以清楚地了解火场事件的状态和消防队员正在实施的救援服务的进展情况。

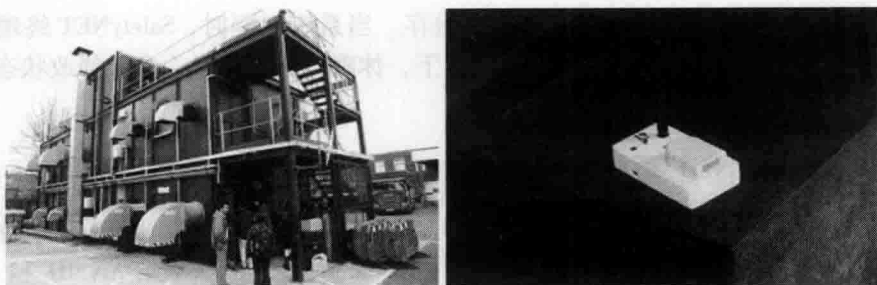


图 14.10 用于现场实验的培训建筑物及部署在其内的无线传感器节点

14.7 小结

SafetyNET 是一个实时、快速响应的系统，旨在当火灾事故发生时，通过提供建筑物和灾害信息，为消防和救援服务（FRS）相关人员提供帮助。这些信息包括对火灾和位于应急现场的救援人员的监控，以及提供平面图和关键的环境数据。SafetyNET 系统的创新之处使其与传统的火灾报警系统不同，它引入一个高度灵活的 WSN。将低成本和低耗能的环境传感器与位置跟踪传感器结合在一起，外加电池驱动无线传输模块的运行，一个正确编程的 WSN 因为不需要布置电缆，可以很容易地部署在建筑物内部任何需要的位置。先进的 Ad-hoc 无线通信协议的使用也将产生有效覆盖。如果主供电电源被切断，作为应急的结果，那么 WSN 将是唯一可用的系统来监控建筑物内部环境和进入内部的消防队员的移动。网络可以收集的所有信息对工作在消防车上的信息处理系统都是可用的。这些信息随后提供给建筑物外现场指挥官，从而拥有最新、最全面的信息，负责整个火灾救援行动。

本章综述了 SafetyNET 系统，包括其系统架构、硬件设备、移动消防车网络和 SafetyNET WSN。所有的设计都是基于本书前几章介绍的原则完成的。

参考文献

Yang, L.: On-site information sharing for emergency response management. J. Emergency Manage. **15**(5), 55–64 (2007)

Yang, S.H., Frederick, P.: SafetyNET—a wireless sensor network for fire protection and emergency responses. Meas. Control **39**(7), 218–219 (2006)

Yang, L., Prasanna, R., King, M.: On-site information systems design for emergency first responders. J. Inf. Technol. Theor. Appl. **10**(1), 5–27 (2009)

第15章 结　论

关键词：无线传感器网络　远程监控　远程控制　移动目标跟踪

15.1 总结

WSN 是计算机科学和电子工程领域新兴的研究课题之一。WSN 的应用覆盖了从自然监测到环境感知，从军事到监控的广阔范围。通过无线传感器节点间的协作，可以获得 WSN 提供的服务。WSN 提供的服务包括监控、跟踪、报警和“按需”提供信息（Roman 等，2007）。传感器节点能连续监测周围环境的参数，如房间内的温度。传感器能实时跟踪货物的位置、重要的设备和人，识别运动中的人和物。传感器还能够连续监测某种物理状况，当异常状况发生时，对系统用户自动报警。WSN 也可以作为数据源提供服务，并通过“按需”提供的信息查询某个环境参数的实际大小（Shorey 等，2006）。这些服务使得无线传感器和 WSN 非常有利于自然现象监视、环境变化侦测、安全控制、交通流量评估、军事应用监视及战场上的盟军部队的跟踪。

设计和实现 WSN 的主要挑战是在自配置和自维护方面，以及传感器节点在存储、能量、苛刻的应用环境、数据处理能力和寿命方面极度有限的资源。这些新的苛刻的和非传统的约束，使得传统的网络设计方法不再适用于 WSN。本书主要为读者介绍了 WSN 在设计和实现方面的基本问题和解决方案，包括传感器节点硬件设计、嵌入式软件设计、WSN 的路由算法、汇聚节点的位置布局、互扰抑制、数据融合和安全防御。进一步的，本书也介绍了室内定位跟踪、物流管理、IoT 等应用技术。此外，本书有两个实际应用：SafetyNET 和 IndeedNET。需要说明的是，针对设计和实现 WSN 的众多问题，本书并没有给出所有的解决方案。其中的一些问题很难给出通用的解决方案，因此还需要给出指定应用的解决方案。

15.2 未来发展研究展望

目前，大多数商业 WSN 的解决方案都是采用电池驱动并基于 IEEE 802.15.4 标准的。该标准为低能耗、低速率通信定义了 PHY 层和 MAC 层。WSN 大规模部署的最大障碍是各传感器节点的能量限制。在许多场景中，传感器节点在休眠模式下花费大量时间来节能，这通常是难以接受的。为了克服这个最大的障碍，能量收集技术可以提供一个解决方案。但是它成本高、设备大，对于大多数应用是不切实

际的，因为传感器网络是由许多节点构成的。在能量收集工程研究中，任何突破都会通过更实际的应用来扩大 WSN 的市场。

基于 RFID 的 WSN 可以在物理世界和数字世界之间架起一座桥梁。与因特网连接的 WSN 可以感知全球的目标环境或物体，这也是 IoT 的主要目标之一。在 IoT 这个领域还有许多挑战性课题。第 12 章仅对 IoT 进行了简单介绍。IoT 正在成为一个热门的研究领域（Atzori 等，2010；Yang 等，2013）。

第 8 章简要介绍了 WSN 的网内数据处理。近年来，基于电池驱动的传感器节点由于能量受限引起了关注（Gaber 等，2009；He 等，2013）。网内数据处理需要新的以数据为中心的路由机制，也需要重新考虑传统网络和数据库的接口分层问题（Govindan 等，2002）。

最后，WSN 最大的机遇就是大规模的实际应用。本书阐述了作者亲身经历的研究工作和应用实例。本书对重要问题的任何微小改进都将有助于推动 WSN 的发展。

参考文献

Atzori, L., Iera, A., Morabito, G.: The internet of things: a survey. Comput. Netw. **54**, 2787–2805 (2010)

Gaber, M.M., Roehm, U., Herink, K.: An analytical study of central and in-network data processing for wireless sensor networks. Inf. Process. Lett. **110**, 62–70 (2009)

Govindan, R., Hellerstein, J., Hong, W., Madden, S., Franklin, M., and Shenker, S.: The sensor network as a database, Technical Report 02-771, Computer Science Department, University of Southern California (2002)

He, W., Yang, S.H., and Yang, L.: NMCA: Neighbour-aware multiple-path clustering aggregation in wireless sensor networks, IEEE International Conference on Networking, Sensing and Control, Évry, France, 10–12 Apr (2013)

Roman, R., Alcaraz, C., Lopez, J.: The role of wireless sensor networks in the area of critical information infrastructure protection. Inf. Secur. Tech. Rep. **12**(1), 24–31 (2007)

Shorey, R., Ananda, A., Chan, M.C., Ooi, W.T.: Mobile, Wireless, and Sensor Networks. Wiley, Hoboken (2006)

Yang, L., Yang, S.H., and Plotnick, L.: How the internet of things technology enhanced emergency response operations. Technol. Forecast. Soc. Change **80**(9), 1854–1867 (2013)

名词术语

A

Acknowledgment packet (ACK)　确认数据包
Active tag　有源电子标签
Adaptive radio channel allocation　自适应无线信道分配
Address management　地址管理
Ad hoc On-demand Distance Vector (AODV)　无线自组网按需平面距离矢量
Advanced encryption standard (AES)　高级加密标准
Application layer　应用层
Application Programming Interfaces (API)　应用程序接口
Asymmetric key cryptography　非对称密钥加密

B

Bit Error Rate (BER)　误码率
Bit rate　比特率
Broadcasting　广播

C

Carrier-Sense Multiple Access with Collision Avoidance (CSMA-CA)　具有冲突避免的载波侦听多路访问
Centroid Localization　质心定位
Cipher Block Chaining (CBC)　密码分组链接
Clear Channel Assessment (CCA)　空闲信道评估
Cluster-Head (CH)　簇头
Cluster-tree routing　簇树路由
Code Division Multiple Access (CDMA)　码分多址
Coexistence　共存
Coordinator　协调器
Counter Mode Encryption (CTR)　计数器模式加密
Coverage　覆盖
Cryptography　密码学
Cyber-Physical Systems (CPS)　信息物理融合系统

D

Data Advertisement (ADV) 数据广告
Data (DATA) 数据
Data fusion 数据融合
Data link layer 数据链路层
Data mining 数据挖掘
Data post-processing 数据后处理
Data pre-processing 数据预处理
Data Request (REQ) 数据请求
Denial of Service (DoS) attack 拒绝服务攻击
Direct Sequence Spread Spectrum (DSSS) 直接序列扩频
Domain Name System (DNS) 域名系统
Domain Sensor Name Server (DSNS) 传感器域名服务器
DoS Defence Server (DDS) DoS 攻击防御服务器
Dynamic channel selection 动态信道选择
Dynamic sink node 动态汇聚节点

E

Embedded software 嵌入式软件
Energy-aware 能量感知
Energy Detection (ED) 能量检测
Energy scavenging 能量捕获
Event detection 事件检测

F

File Transfer Protocol (FTP) 文件传输协议
Fingerprint 指纹
Flat routing protocols 平面路由协议
Flooding protocol 泛洪协议
Frequency division 频分
Frequency Division Multiple Access (FDMA) 频分多址
Frequency-Hopping Spread Spectrum (FHSS) 跳频扩频
Frequency offset 频段分离
Full-Function Device (FFD) 全功能设备

G

Geographic Adaptive Fidelity (GAF) 地理自适应保真

Global Positioning System (GPS)　全球定位系统

H

Hardware design　硬件设计
Hierarchical routing protocols　分层路由协议
Home automation　家居自动化
Home automation devices　家居自动化设备
Home Automation Systems (HAS)　家居自动化系统
Home gateway　家居网关
Humanitarian logistics management　人道救援物流管理
Hybrid RFID　混合 RFID
HyperText Transfer Protocol (HTTP)　超文本传输协议

I

Industrial, Scientific research and Medical applications (ISM)　工业、科研和医疗应用
In-network aggregation　网内整合
Inter-cluster　簇间
Interference　互扰，干扰
International Organisation for Standardization (ISO)　国际标准化组织
Internet of Things (IoT)　物联网
Intra-cluster　簇内

K

Key cryptography　密钥加密

L

Local Area Network (LAN)　局域网
Lifetime　寿命
Link Quality Indication (LQI)　链路质量指示
Logical Link Control (LLC)　逻辑链路控制
Low Energy Adaptive Clustering Hierarchy (LEACH)　低能耗自适应分簇路由协议
Low-Rate Wireless Personal Area Network (LR-WPAN)　低速率无线个人局域网

M

Media Access Control (MAC) layer　媒体访问控制层
Mesh topology　网状拓扑
Metropolitan Area Network (MAN)　城域网

Mobile sink node　移动汇聚节点
Multi-hop　多跳
Multiple mobile targets tracking　多移动目标跟踪

N

Network command transmission and reception　网络命令的发送和接收
Network establishment announcement　网络构建公告
Network initialization　网络初始化
Network layer　网络层

O

Open System Interconnection (OSI)　开放系统互联

P

Packet Error Rate (PER)　误包率
Passive tags　无源标签
Personal Area Network (PAN)　个人局域网
Personal Area Network Identifier (PAN ID)　个人局域网标识
Physical (PHY) layer　物理 (PHY) 层
Power supply　电源

Q

Quality of Service (QoS)　服务质量

R

Radio channel assessment　无线信道评估
Radio Frequency (RF)　无线电频率
Radio Frequency Identification (RFID)　射频识别
Real-time Locating System (RTLS)　实时定位系统
Received Signal Strength (RSS)　接收端信号强度
Received Signal Strength Indicator (RSSI)　接收端信号强度指示
Reduced-Function Device (RFD)　精简功能设备
Remote Home Server (RHS)　远程家居服务
RFID reader　RFID 读取设备
RFID tag　RFID 标签
RHS client　远程家居服务客户端
Route Error (RERR)　路由错误

Route Repliy (RREP)　路由应答
Route Request (RREQ)　路由请求
Routing protocol　路由协议

S

Secure Ad-hoc Fire Emergency Safety NETwork (SafetyNET)　消防安全应急响应无线自组网络
Secure Socket Layer (SSL)　安全套接层
Security attack　安全攻击
Security mechanism　安全防御机制
Security service　安全防御服务
Semi-active tags　半有源标签
Sensor driver　传感器驱动
Sensor Protocol for Information via Negotiation (SPIN)　基于协商的传感器路由协议
Sensor Service Publishers (SSP)　传感器服务发布
Service-oriented Architecture (SoA)　面向服务的体系结构
Service Specific Convergence Sublayer (SSCS)　特定服务汇聚子层
Signal to Interference and Noise Ratio (SINR)　信干噪比
Signal-to-Noise Ratio (SNR)　信噪比
Simple Mail Transfer Protocol (SMTP)　简单邮件传输协议
Sink node　汇聚节点
Spread spectrum　扩频
Static sink node　静态汇聚节点
Superframe structure　超帧结构
System-on-Chip (SoC)　片上系统

T

Tempo-spatial　时空
Time Difference of Arrival (TDOA)　到达时间差
Time Division Multiple Acces (TDMA)　时分多址
Time of Arrival (ToA)　到达时间
Time synchronization　时间同步
Transmission Control Protocol (TCP)　传输控制协议
Transmission range　传输范围
Transport layer　传输层
Triangulation approach　三角定位法

U

User Datagram Protocol (UDP)　用户数据报协议

User data transmission/reception　　用户数据发送/接收

V

Virtual Home（VH）　　虚拟家居

W

Wireless communication　　无线通信
Wireless Sensor Network（WSN）　　无线传感器网络
WSN protocol stack　　无线传感器网络协议栈

Z

ZigBee　　一种低速短距离传输的无线网络协议
ZigBee topologies　　ZigBee 拓扑结构

国际视野　科技前沿

国际信息工程先进技术译丛

《无线传感器网络——原理、设计和应用》
《IPv6部署和管理》
《虚拟网络——下一代互联网的多元化方法》
《下一代融合网络理论与实践》
《认知视角下的无线传感器网络》
《移动云计算：无线、移动及社交网络中分布式资源的开发利用》
《Android系统安全与攻防》
《内容分发网络》
《计算机网络仿真OPNET实用指南》
《移动无线信道》（原书第2版）
《LTE-Advanced：面向IMT-Advanced的3GPP解决方案》
《声学成像技术及工程应用》
《认知无线电通信与组网：原理与应用》
《LTE/SAE网络部署实用指南》
《网络性能分析原理与应用》
《云连接与嵌入式传感系统》
《IP地址管理原理与实践》
《自组织网络：GSM，UMTS和LTE的自规划、自优化和自愈合》
《实现吉比特传输的60GHz无线通信技术》
《LTE自组织网络（SON）：高效的网络管理自动化》
《UMTS中的LTE：向LTE-Advanced演进》（原书第2版）
《无线传感器及执行器网络》
《UMTS中的WCDMA－HSPA演进及LTE》（原书第5版）
《认知无线电网络》
《网络融合——服务、应用、传输和运营支撑》
《UMTS中的LTE:基于OFDMA和SC-FDMA的无线接入》
《高性能微处理器电路设计》
《吉规模集成电路互连工艺及设计》
《高级电子封装》（原书第2版）
《基于4G系统的移动服务技术》
《移动无线传感器网——技术、应用和发展方向》
《UMTS蜂窝系统的Q0S与Q0E管理》
《UMTS-HSDPA系统的TCP性能》
《基于射频工程的UMTS空中接口设计与网络运行》
《未来UMTS的体系结构与业务平台：全IP的3GCDMA网络》
《环境网络：支持下一代无线业务的多域协同网络》
《基于蜂窝系统的IMS—融合电信领域的V0IP演进》
《蜂窝网络高级规划与优化 2G/2.5G/3G/——向4G的演进》
《微电子技术原理、设计与应用》
《多电压CMOS电路设计》
《P2P系统及其应用》
《IPTV与网络视频：拓展广播电视的应用范围》



机械工业出版社微信服务号

上架指导　工业技术／通信工程



ISBN 978-7-111-49570-3

定价　68.00元